THE OFFICE OF THE NATIONAL COORDINATOR
FOR HEALTH INFORMATION TECHNOLOGY

MOBILE DEVICES ROUNDTABLE: SAFEGUARDING HEALTH INFORMATION

REAL WORLD USAGES AND REAL WORLD PRIVACY & SECURITY PRACTICES

Washington, D.C.

Friday, March 16, 2012

ANDERSON COURT REPORTING
706 Duke Street, Suite 100
Alexandria, VA 22314
Phone (703) 519-7180 Fax (703) 519-7190

PARTICIPANTS:

Introduction/Housekeeping Remarks:

KATHRYN MARCHESINI, JD
U.S. Department of Health and Human Services
Office of the National Coordinator for Health Information Technology

Welcoming Speaker:

FARZAD MOSTASHARI, MD, ScM
U.S. Department of Health and Human Services
National Coordinator for Health Information Technology

PANEL I: SETTING THE FEDERAL STAGE: CURRENT REGULATORY FRAMEWORK, GUIDANCE, STANDARDS, AND TOOLKITS FOR PROVIDERS AND OTHER HEALTH CARE DELIVERY PROFESSIONALS USING MOBILE DEVICES

Moderator:

JOY PRITTS, JD
U.S. Department of Health and Human Services
Office of the National Coordinator for Health Information Technology
Chief Privacy Officer

Panelists:

TIM GRANCE
National Institute of Standards and Technology (NIST)
Computer Security Division, Senior Computer Scientist

CORA TUNG HAN, JD
Federal Trade Commission (FTC)
Attorney, Division of Privacy and Identity Protection

PARTICIPANTS/PANELISTS (CONT'D):

GERALDINE MATISE, JD
Federal Communications Commission (FCC)
Chief, Policy and Rules Division
Deputy Director, Office of Engineering and Technology OET)

SUSAN McANDREW, JD
U.S. Department of Health and Human Services
Deputy Director, Office for Civil Rights (OCR)

BAKUL PATEL, MS, MBA
Food and Drug Administration (FDA)
Policy Advisor, Center for Devices and Radiological Health

PANEL II: REAL WORLD USAGES OF MOBILE DEVICES BY PROVIDERS AND OTHER HEALTH CARE DELIVERY PROVIDERS

Moderator:

JON WHITE, MD
Agency for Healthcare Research and Quality (AHRQ)

Panelists:

JACOB DELAROSA, MD
Cardiovascular Surgeon, Idaho State University
Chief of Cardiothoracic and Endovascular Surgical Services, Portneuf Medical Center

LISA A. GALLAGHER, BSEE, CISM, CPHIMS
Senior Director of Privacy and Security, Healthcare Information and Management Systems Society (HIMSS)

STEVEN JEFFERY HEILMAN, MD, FACEP
Chief Medical Information Officer, Norton Healthcare

PARTICIPANTS/PANELISTS (CONT'D):

MERI SHAFFER, RN
Clinical Systems Analyst,
Montefiore Home Care

CHRISTOPHER H. TASHJIAN, MD, FAAFP
President, River Falls,
Ellsworth & Spring Valley Medical Clinics

PANEL III: REAL WORLD MOBILE DEVICE PRIVACY AND SECURITY PRACTICES, STRATEGIES, AND TECHNOLOGIES

Moderator:

DAVID HOLTZMAN, JD, CIPP/G
Health Information Privacy Specialist
U.S. Department of Health and Human Services,
Office for Civil Rights (OCR)

Panelists:

SHARON FINNEY, CISM, CISSP
Corporate Data Security Officer, Adventist Health System

JAMES FRENCH, MD
Executive Medical Director, Hospitalist Program,
Mercy Medical Center

TERRELL W. HERZIG, MSHI, CISSP
Information Security Officer,
University of Alabama at Birmingham (UAB) Health System

ADAM KEHLER, BCSc, CISSP, CHP
HIT Privacy and Security Specialist, Quality Insights of Pennsylvania -
Regional Extension Center (REC) for Pennsylvania East and West

PARTICIPANTS/PANELISTS (CONT'D):

MICKY TRIPATHI, PhD, MPP
President and Chief Executive Officer,
Massachusetts eHealth Collaborative (MAeHC)

Closing Remarks:

JOY PRITTS, JD
U.S. Department of Health and Human Services
Office of the National Coordinator for Health Information Technology
Chief Privacy Officer

* * * * *

P R O C E E D I N G S

(8:30 a.m.)

MS. MARCHESINI: Good morning. I'm Kathryn Marchesini with ONC's Office of the Chief Privacy Officer. We've been anticipating this event for months. Thank you for joining us.

We have a great turnout. We had over 1,500 registrants who will be participating by Web cast as well as in-person and audio. We're here today to talk about mobile devices, protecting and safeguarding health information, but before we dive into the discussion, there's a few housekeeping logistics that I just wanted to go over.

Anyone who leaves the Humphrey Building without an HHS badge will need to go back through security to enter the event. Restrooms are located on this floor to the left of the stage on the other side of the elevator. You take another left. Also, please silence all electronic devices. We ask that if you talk on the phone during the event, please leave the event area. The event's actually being recorded so your conversation would be forever with us.

As you know, during the panel discussion, we will welcome questions from the audience. If you would like to submit a question and you're participating in the actual event room, please write your question on one of the notecards that were provided. During today's event, please raise your hand. One of the floaters in the room will collect your card. Will the individuals helping with the public comment period please raise your hand? There's an individual and another individual. If you're joining us by Web cast or phone, please submit your questions via privacyandsecurity@hhs.gov as well as Twitter with the hashtag #mhealth. For all questions, floaters will submit them to the moderator to introduce into the discussion as time permits. If you have general comments about today's event, please make them online via the mobile device roundtable web site.

Now, to move to today's program. Ladies and Gentlemen, our opening speaker this morning is well-known to us and others in the health care industry. In fact, he's the National Coordinator for Health IT across the United States. In a former life, he was Assistant

Commissioner for the Primary Care Information Project at the New York City Department of Health and Mental Hygiene, where he facilitated the adoption of prevention-oriented HIT by over 1,500 providers in underserved communities. He also led the CDC-funded New York City Center of Excellence and Public Health Informatics, as well as an AHRQ-funded project focused on quality measurement at the point of care. I don't want to take another of the event's time, so, to kick things off today's discussion, please join me in welcoming Dr. Farzad Mostashari. (Applause)

DR. MOSTASHARI: Hello, good morning.

AUDIENCE: Good morning.

DR. MOSTASHARI: How is everybody? How is everybody online? Hello.

So, I tell this story of being at my health clinic, getting my prescription refilled, and admitting to the provider that if I try to take the pill as it says on the bottle at night, I kind of forget. And I take it about 60, 70 percent of the time. Bad patient. But if I take it in the morning, I can fit it into my

routine better and I take it most of the time, but the pill says take at night and I said to the pharmacist, is it really that important if I take it at night or in the morning, and the pharmacist said yes, take it at night. And I said what's the half life? Bad patient. And the pharmacist in his starched-white coat with his badge with the computer screen between him and me goes into his pharmacy information system, starts clickety-clacking. I can't see what he's doing. But as the seconds tick by, as he's trying to find the half-life, I'm thinking it, he's thinking it, he's looking at the mouse, and now the expectation is right, that the information's going to be found and both of us know and he says aw, heck, let me just Google it. (Laughter) Right?

So, that's when what we have in our pocket is ubiquitous, we always have it with us. When it's connected, when that device taps into the world's knowledge and when it's a platform where it's not just a device that does one thing, where it's a platform on which some of the same data, when you can have a near

infinite number of applications that could run on that device, on that hardware, that's when disruptive innovation in the best sense of the word is unleashed. Ubiquitous, connected platform. Ubiquitous, connected platform. And the use of these is skyrocketing, as everybody knows, and one of the interesting things about this is that like many disruptive innovations, it starts in one side of the market, the lower cost side of the market, and then it comes in and takes over the higher cost, and in our case, it's consumer technology coming into institutional technology, medicine, one of the most conservative bastions for adoption of technology with good reason in many cases, because the stakes are literally life and death.

So, whereas it used to be that it was investments in NASA and military and very sophisticated systems that eventually found their way in Teflon pans, right, that the consumer used, now the massive amount of research and development going on in the consumer technology field is moving innovation the other way. When I heard the military was using modified video game

controllers for their aerial, unmanned vehicles and the same thing is happening medicine. Like it or not, increasingly, mobile devices meant for a consumer technology marketplace are so usable, so pleasurable, so ubiquitous, so connected platforms that they are being increasingly used in health care, like it or not, like it or not. And, so, we have to think not only about the possibilities, but also the potential perils.

Ubiquitous means you always have it with you, which means you can lose it at any time. Connected means it's not just the data on the device that could be compromised. It's the data in the cloud that could be compromised. Platform means different applications have to be able to access the same data and those, as we've seen and heard recently, there are vulnerabilities that can be introduced there, where an application that you had no idea was accessing certain parts of your information is now tapping into your contacts, your locations. So, each of those characteristics creates risks for privacy and security when these applications, these devices are being used not just in the consumer

technology space, but moving now into health information and the health care space.

And, so, we do what we do at the Office of the National Coordinator. We get the smartest people in an open process to help us be smarter, to help us learn, and we have used different ways, we have many of you here and we have, you heard, over 1,000 folks online and on the phone and participating in the broader conversation that we want to have today about how can we make sure that we understand the issues of privacy and security of mobile devices, that we understand what the current legal framework is for mobile devices that access, store, and transmit health information, we understand how the real world usage of these devices is taking place by providers and other health care delivery professionals to understand what their expectations and attitudes are, to understand what they want, what are the needs of the users, and understand what are the existing and emerging best practices around safeguarding health information on mobile devices. And we seek comment.

I should also note that there's a connection to the meaningful use of electronic health records in the Stage Two Meaningful Use Proposed Rules. We're in the comment period now. We would love your comments on this aspect, among others. CMS in their rule proposed that particular attention be paid to encryption as part of the security assessment and in our certification rule, we proposed that if data is kept on mobile devices that the electronic health record software by default encrypt that information. These are small pieces of a much larger question about how can we ensure that we have done everything we can to maintain the privacy and security of health information wherever it sits?

So, in conclusion, the promise of the technology of those ubiquitous, those connected platforms and not just the risks, but also the opportunities, we would like to hear from you about. It's possible that in the same disruption lie the seeds of dramatic increases in ability to maintain privacy and security.

One of the most difficult issues we face is

around authentication around individuals, making sure that it's the right person who's accessing that information, and people have talked about two-factor authentication, not just something you know, but something you are, something you have, being a necessary component of increasing privacy and security online. Well, if we do all have something in our hands, that, too, could serve as a second factor for authentication. So, I'd like us to engage today on a really far-ranging discussion of the current state of the possibilities and I have every confidence that by having these open dialogues with you, we're going to achieve the best product possible for the American people. Thank you.

(Applause)

I'd like to introduce Joy Pritts, who is the Chief Privacy Officer within Office of the National Coordinator, but really has been the conscience for privacy and security in everything that we do and has been a tremendous advocate and really effective coordinator in her own right of a lot of the discussions around privacy and security we have both with the

private sector and also within our federal families.

Joy?

MS. PRITTS: Thank you, Farzad. When Farzad calls me "the conscience," what he really means is that nag that is always there in all the conversations.

Welcome to you all. We're going to get started now with our first panel. We thank Farzad, Dr. Mostashari, for his wonderful introduction to this topic. It gives a good background for how these items have moved from the consumer world and are rapidly moving into the health care sector, and they're doing so in a vacuum. There is a current federal role here and our first panel is going to talk about it. So, please come up.

Our first panel is going to set the federal stage and discuss the current regulatory framework, guidance, standards, and toolkits for providers. And we will be focusing today, as Dr. Mostashari mentioned, on the privacy and security of mobile devices as they are used in the health care sector by health care providers for providing care.

So, what we're going to do here is we're going to talk, we're going to have each member of our federal panel discuss a little bit about who they are and the agency that they are with and in particular focusing on how that agency interacts with mobile devices and health care information, and, in particular, the privacy and security of that information because many of these agencies have a much broader mandate. So, we have with us today members from -- and I will let them all introduce themselves -- the FCC, the FDA, the FTC, OCR/HHS, and NIST. Now, if that's not an alphabet soup, I don't know what is. But we will start here with Geraldine Matise, who is with FCC and, Geraldine, why don't you talk to us a little bit about what the FCC does in general and in specific what it does with respect to mobile devices and how it might interplay with health care and security in specific.

MS. MATISE: Good morning. I'm Geraldine Matise with the FCC. I'm an attorney that works in the Office of Engineering and Technology at the FCC. Most of the people in my office are engineers. We have a few

attorneys and some economists, as well, but the Federal Communications Commission, its charge under the Communications Act of 1934 is to regulate interstate and international communications by radio, television, wire, satellite, and cable. It's a very broad charge. Our jurisdiction extends to non-federal users of spectrum in the 50 states, the District of Columbia, and the U.S. possessions.

In terms of what's relevant for this workshop today is we manage the radio frequency communication to ensure that RF devices operate efficiently and without interference and we do this in a number of ways. For example, we decide which frequency bands are to be used by different services. Some people refer to it as the idea of good fences make good neighbors. We establish technical rules for the operation of RF devices, we authorize the RF equipment to make sure that it's compliant with our rules, our technical rules, in particular, and we authorize users of different equipment because it can vary. We can authorize individuals or we authorize network service providers,

as appropriate, depending on what the services are.

In the health area, we basically are engaged in two primary ways. One is that we authorize a variety of RF-based medical devices under Part 95 of our rules, and these include implanted medical devices, such as heart pacemakers or defibrillators, and we also authorize patient monitoring devices, such as wireless medical telemetry.

In terms of medical mobile devices, which we're talking about here, what we basically do is we authorize carriers whose networks are used by a wide variety of these devices to access, store or transmit information, including health information, and we also established technical rules that are used by Wi-Fi or other similar networks for very short transmissions. These may or may not be integrated with the carrier's network. Something like Wi-Fi, for example, if you have a wireless router at home, that's something that you just buy yourself and install. So, that's pretty much the broad scope of what we do.

MS. PRITTS: So, Geraldine?

MS. MATISE: Yes.

MS. PRITTS: Can I ask you a question on this? Does the FCC require encryption or any other security measures for any devices?

MS. MATISE: Generally, no. We don't require that, but we know that most device manufacturers in the Wi-Fi area make a functionality available and carriers will protect their networks in various ways. They do this to improve the quality of service.

The Communications Act does have two very broad prohibitions, which is not a requirement on the carriers, per se, it's actually required on those of us as users. People are not to intentionally interfere with a radio transmission; in other words, jamming. It's basically illegal in this country to jam a radio signal and we also, there are prohibitions on intercepting radio communications and divulging the content, and that's a provision that's particular to carriers.

Historically, again, the Communications Act being as old as it is, the two broad areas that it was

set up to regulate were broadcast and common carriage. Broadcasters do control the content on their networks, carriers are supposed to provide service on a non-discriminatory basis. So, they are not supposed to discriminate, they're supposed to carry everything. But people are not supposed to intercept that unless they have a lawful instrument, such as a trap and trace or a surveillance that law enforcement uses.

MS. PRITTS: Okay, so, to summarize with respect to security, one aspect of security is data integrity and one of the things that FCC does, the rules do, is say that the information as it is sent to the receiver may not be intercepted --

MS. MATISE: That's right.

MS. PRITTS: And another issue is availability of the information. So, the jamming is also prohibited under FCC.

MS. MATISE: That's right.

MS. PRITTS: Okay. So, we will now turn to the FDA, which has more of a health focus. As you can see, the FCC has a very broad focus, but it does impact

on health and mobile devices and the FDA has more of a health focus and we will have Mr. Bakul Patel.

MR. PATEL: Thank you, Joy. Good morning, everybody. And a great introduction from FTC.

I'd like to start off with FDA's mission has been to promote and protect public health. So, I'll start from there and then I'll walk towards how we fit in with the privacy and security of technology involving health care or health of patients.

We start off with the mission of promoting and protecting, and from there, we look at balancing the benefits and risk of technology used in health care settings, used for medical device purposes or medical intentions. Again, I'm trying to stay away from a whole lot of technical and term of arts that you use in the FDA, but mostly it boils down to if it's used for patients for curing, mitigating, treating disease, that's where our jurisdiction lies, and I didn't say it in the whole definition of a medical device, but that's really the gist of it. And technologies can do this; many forms of technologies can do this. We continually

look at risk to patients and, again, focusing from the safety towards the patients and public health.

The other part of our mission is effectiveness of technology in actually treating, curing, mitigating disease in patients. So, very much health-focused, risk to patients is really what a lot of our focus is. And if you can imagine the different types of risks that exist in medical devices and other technologies, privacy and security is part of that. We look at privacy and security from the risk to patient's perspective and we ask questions for people regarding does jamming cause risk to patients? Is it going to hurt patients at the end of the day?

So, giving you a little bit of background of what we have been working on is we are working on developing policies that are smart to advance this field. We totally understand and we are encouraged by the innovation that's happening in the mobile area. We are also excited about the fact that solutions that were once in a very specific setting is now being changed into technology agnostic or location agnostic solutions

that are going in the health field. We are taking all of that into consideration. We are looking at non-traditional ways to tradeoff between benefits and risk, which is a big factor for us to look at how we oversee medical devices and what are the requirements we put on manufacturers of those devices? That's really where we focus on.

Last year, we released a draft guidance on how and what types of mobile medical apps would be overseen by FDA and one of the things we've done there is we looked at a very small portion that becomes -- a portion of those mobile apps that becomes -- either by attaching sensors or other activators to a mobile platform of a computer to turn it into a traditional medical device. And we can talk a lot more about the examples, but those are one of the things.

There are many things happening in this area in mobile perspective where knowing where people are is also helping people, patients, mitigate or avoid certain risks or certain treatments or use certain treatments to use mobile technology as part of that solution for care.

And, having said that, I will probably stop there with examples because I could probably go on forever.

MS. PRITTS: Okay, so, to summarize the FDA focuses, in our area, on the use of the mobile device as a medical device and the privacy and security, particularly the security of that is measured, taken into account in weighing the cost and benefits to the patient.

MR. PATEL: Correct.

MS. PRITTS: Okay, great.

So, if we can turn to our next panelist who is Cora Tung Han, who is with the FTC, and, as you can see, as I know you all know, FTC is much broader than health-focused. So, Cora, could you give us a little discussion about the FTC plays a role in this area?

MS. HAN: Sure. Thank you very much and good morning.

So, the FTC's core enforcement statute is Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices. So, an act or practice is deceptive if it involves a false or misleading claim or

one that omits a material fact, and an act or practice is unfair, if it causes or is likely to cause substantial harm to consumers, that is not reasonably avoidable and that is not outweighed by countervailing benefits to consumers or to competition.

So, as Joy mentioned, this is a very broad mandate and it applies regardless of what medium representation might be made. So, whether or not something is said in print, television, a desktop computer, or a mobile device, these same rules of the road apply and the FTC has taken enforcement action in the mobile area and I'll just give you two very quick examples. One involved a case against marketers of apps that claimed to treat acne through a light emitted from the device if you held it close to your face and we alleged that those claims were unsubstantiated. In addition, we had also another recent enforcement action against the developer of a peer-to-peer files-sharing app that caused consumers to unwittingly share sensitive and personal information on their mobile device. So, we have a broad number of actions and they apply regardless of the arena.

MS. PRITTS: So, but one of the key elements that helps bring a mobile device within the purview of the FTC is if they actually make representations about what they do.

MS. HAN: That's right, and those representations can really be a number of different ones. So, it can be in the privacy policy of an app developer or of a platform. There's a little privacy policy, a picture up there, but it can also be something like a privacy setting. So, we have had enforcement actions where we alleged that well, a privacy setting that tells consumers that their information will be kept private, if it doesn't actually do that, that’s going to be a problem for us under Section 5. And, in addition, representations can also be beyond the setting and the policy, other statements made on a Web site or on a mobile device that people see.

MS. PRITTS: Okay, thank you very much.

I’m going to pause here just for a second. As Kathryn mentioned, we will be taking questions both from the in-person audience and the audience that is on

the Internet. So, if you do have questions or comments, please write them down and you can raise your hand, you can get a card and you can pass them in here and we will use them to facilitate our question and answer period.

Okay, given that, we're going to turn back to a health focus here and I'd like to ask Susan McAndrew of the Office for Civil Rights here at HHS to explain to us a little bit about how the Office for Civil Rights -- what your role is in this area.

MS. McANDREW: Thank you, Joy, and in honor of the St. Patty's Day, I will take the mike with the green wrapper. Very good. I appreciate that.

MS. PRITTS: Very good. See, I dressed for the occasion. I just want to point that out.

MS. McANDREW: The Office for Civil Rights does have jurisdiction under the Health Insurance Portability and Accountability Act, lovingly called HIPAA, to protect the privacy and security of health information when it is held and maintained by particular entities in the health industry, such as health care providers, health plans, and their business associates.

So, we have a very particular focus and if Joy is the privacy "conscience" of the enterprise, then OCR can have the role of cop. So, we do have an enforcement role with respect to privacy protections.

With regards to mobile devices, it is clear that these are a part of the electronic systems and enterprise within a doctor's office or a health plan, and, so, they do come within the ambit of the HIPAA Security Rule and are subject to all of those protections, including primarily it is important that entities recognize that and include them as part of their risk assessments as they go forward and that they do take the same kinds of protections with regard to those devices as they would to the main computer systems within the enterprise so that if the device is receiving and transmitting protected health information, that is identifiable information about patients, then they need to consider whether or not that information in transmission and if it's stored on the device needs to be encrypted. This is not a hard and fast mandate, but if it's reasonable to do so and they can reduce the risk

of the information, then they should do that or something similar to that.

There are other kinds of protections, including making sure that the users of the system are authenticated and that they have controls about who can access the system. As Farzad mentioned in his opening remarks, these devices have many roles and many vulnerabilities, including it's not just the information that is sent to and from these devices, but because of the device, it may present access to other systems and those kinds of controls need to be recognized and protected against should the device fall into unauthorized hands, and we know how often Blackberrys, laptops, smartphones, and other things go missing, are the object of theft, and when that happens, we cannot necessarily cut down on that kind of theft, but it is totally within the control of entities to make sure that when that kind of theft or loss occurs that the information that is on that device or to which that device allows access is not also put into jeopardy so that all that you have lost is the actual device itself.

These devices are subject to our breach notification requirements so that if these devices are lost or stolen and there is information that is stored on the device, the entity is required to notify individuals whose information has been placed in jeopardy about that event and they are also required to notify the Secretary when these incidents occur, and many of our breach notifications are the result of these kinds of mobile devices that are lost or stolen. So, it is a frequent occurrence and there are easy ways to protect the information, if not the device itself.

MS. PRITTS: Okay, thank you, Sue.

And we are now going to turn to our final panelist who is with NIST, which has a much broader mandate than health and which unlike most of the other panelists, is not a regulator, but is an agency that provides a lot of guidance. So, if I could please ask Tim Grance to explain a little bit about what NIST does and how it operates on this specific issue, please.

MR. GRANCE: Indeed. Well, thank you for having me. I am from NIST. We are non-regulatory. We

have no foreign policy. We're the nice people in the U.S. Government.

MS. PRITTS: You're here to help us, right?

MR. GRANCE: We just write things down, put it up on the web site, and hopefully, people find it interesting and valuable. So in general let me say NIST is part of the Department of Commerce. We are involved around the idea of measurement and standards, testing, mostly around the idea of physical sciences, like physics, chemistry, material science, and, of course, in computer science. We do things like some of the universal constants. What is a kilogram, what is a second? And, believe me, I have actually carried a kilogram, a reference kilogram and you can imagine me going through security with a reference kilogram. (Laughter) What do you have there? I have a kilogram. A what? (Laughter) Just a kilogram, sir. All right, step aside here. True story.

So, again, we're probably known mostly in the physics area, three Nobel Prizes. My mother thinks it's still possible I might get one. It's not going to

happen, but she still thinks so.

In the area of computer science, we have an information technology lab, several divisions, networking, human interface in various areas. The one I'm in is the Computer Security Division and we write publications on a variety of topics ranging from cryptography, access control, vulnerabilities, cloud computing, the whole spectrum of security things, as well as what I would call on the softer side is this is how a training program might work, this is how risk management works, this is how you would think about doing risk analysis, two more esoteric things in the works about this is how you would model a threat on your particular space or environment, how you would think about that, how we would try to deal with those things.

We operate a very busy and active web site. It gets probably 100 million hits between something called a National Vulnerability Database on the other parts and there's nothing we put up there that's inappropriate, but it still gets a lot of hits from all around the world, frankly, mostly from non-government

actors. And, so, the guidance we write generally gets an orientation towards the federal government, but we try to write it in a language and manner that's accessible by anyone in the world who wishes to read it and comment on it, and we actively encourage people. We really do listen to the comments and we don't maybe sound like it on the phone or anything, but we do listen carefully and handle those comments with great care and deliberation.

So, with that, I'll stop here.

MS. PRITTS: Okay. So, as you can see there are a lot of different federal agencies that are involved in the area where this all intersects and we have a question that came in which is basically why can't just one of you do this? Where is the responsibility going to live? And, so, I'd like the panelists to discuss a little bit about where the potential overlap here is in regulation and how the agencies have worked together a little bit in the past to address some of these issues.

Do you want to start over here?

MR. PATEL: I know you were going to say the same thing.

MS. MATISE: I know. The FCC and the FDA collaborate quite a bit in the area of medical devices, in particular with Bakul. We had a joint workshop about two years ago, which basically dealt with the area of who does what for medical devices and our agencies entered into a memorandum of understanding so that we confer on a regular basis about any number of issues.

MS. PRITTS: Bakul?

MR. PATEL: I'd like to echo that and I'd like to add also one more thing for FTC. We also at FDA collaborate with FTC on areas that overlap in terms of the deception part that Cora mentioned earlier. We have a similar charge on our end which goes back to misbranding of medical devices and misbranding equals misleading and then somewhere it blurs the line between deception and goes over to FTC, then there's no direct harm in certain cases where we either choose to have FTC take action or us, so, we collaborate on that area. Similar to FCC, we also look at implantable medical

devices, what risks exists, and we work together on those aspects of the technologies side, as well as the consumer protection side and patient safety side.

MS. PRITTS: Cora?

MS. HAN: I'd like to echo what has been said. We do coordinate and talk and refer things back and forth and we also try to reduce areas of confusion caused by overlapping jurisdictions.

So, for example, the FTC also has a health breach rule that applies to breaches of sensitive health information for mostly non-HIPAA-covered entities and when we went through that process, we tried to work together to ensure that it was clear as possible and that there was as little overlap as we could manage.

MS. MATISE: I'd like to mention something. It's maybe a little unusual, but in terms of our working with NIST, we actually have had quite a working relationship because they are involved in standards and when we approve devices of all different types, we require the manufacturers to have them tested and there are, of course, a lot of devices today are not

manufactured in the U.S.; they're manufactured overseas, and they're under trade agreements, what we call mutual recognition agreements, that recognize test labs as being qualified to test products in compliance with FCC rules, and NIST has worked very well with us because they can actually do the accreditation process for labs, and we have worked very closely with them for probably over 10 years now on that. So, it's a very valuable role that they play to health agencies like us.

MS. PRITTS: Okay. I've got a next question or, Sue, did you want to comment on that?

MS. McANDREW: Well, I also wanted just to say that with regard to the partnerships that we have in addition to the shared jurisdiction with the FTC and we both did work very closely together to align the regulations on breach, but we really do find the resources in NIST to be a wonderful partner for us. They have helped develop a number of tools that are specific to the HIPAA Security Rule Guides for users and they just have a new tool out, a computer-driven help tool for risk assessment. So, they are a great resource

for us and we also have close relations with the FDA to the extent any of the medical device integrity issues also implicate a Security Rule problem.

MS. PRITTS: So, that's a great segue into -- we see a couple of comments and questions on this, and I'm going to direct this one primarily to Tim and to Sue, which is: How do the mobile devices play into this risk assessment? So, the Security Rule, Sue, requires people who are covered by HIPAA have to conduct a security risk assessment, right?

MS. McANDREW: That's right.

MS. PRITTS: And meaningful use now also requires as one of its elements that people to receive their incentive payments that they attest, that they've actually done that, that they have done that element. And, so, how does this work with mobile devices, do you have to include this in a security risk assessment? Is this part of a system? Tim?

MR. GRANCE: I can give you a set of sort of general rules of thumb I think people should be considering, but we would definitely encourage people to

take an enterprise-wide view or an agency-wide view of their mobile devices. And, in fact, caused me to actually look at my list here. And this is sort of draft, but it's (mike feedback). I must have said something bad in a moment here. (Laughter) We're going to suggest to people you should examine the issues around those devices. What are the threats to those devices? What does it mean to use them? It's important to think about context of use and, of course, the mission benefit you're trying to confer; if you're a government agency, if you're in the private sector, to your business function, what are the issues there? We think people should deploy these devices and have kind of a generalized policy about what you want people to do with them, personal use versus private use. Do you want me to go on or --

MS. PRITTS: No, I have a specific question on this. So, NIST does have mobile security guidance out or something of that nature, is that right?

MR. GRANCE: We have several publications that contribute to that.

MS. PRITTS: Can you get the mike up closer to your mouth, please? Thank you.

MR. GRANCE: We have several publications like that. But there's one in particular that's directly to it, but it's a little dated because it's 2008. That's in the process of being updated. I'm going to hazard a guess that no one should ever quote me on. I would say within the next month or two, that should be out for draft comment.

MS. PRITTS: Okay.

Sue, this one's directed for you, I think, which is people are looking for a little bit of an explanation as to when the Privacy Rule does and doesn't apply. So, for example, if a doctor has a -- assuming that they qualify under HIPAA for all the other things, but, generally, if a health care provider, a doctor has information on a mobile device, that's subject to HIPAA, right?

MS. McANDREW: To the extent the information is identifiable information about a patient, then that information is protected by HIPAA and if the doctor is

using the mobile device as part of his practice and that's how the information got there, then, yes, that information is protected by HIPAA and that device needs to be considered for its security risks.

MS. PRITTS: Okay, so, now, as Dr. Mostashari mentioned earlier, patients are also using these devices a lot to store their own medication. Perhaps, they're looking at their dietary requirements or they're storing information about the exercise they get or even storing information about what their glucose levels are. So, if an individual has a mobile device, is that covered by HIPAA?

MS. McANDREW: The devices that are for the individual themselves, whether it's a mobile device or their home computer, no, HIPAA does not tell the individual what they can or cannot do or must do to protect the information. I mean, clearly, the individual needs to consider the same kinds of risks and protections for the information that they have on their own machines, but HIPAA does not control how an individual uses their own information.

MS. PRITTS: Okay, but I'm going to turn to Cora on that. Just so people get a fuller picture here, if it is the individual's device and they do have medical information on it, that might implicate FTC jurisdiction, is that right?

MS. HAN: That's right because our focus is on consumer protection, so, we're very much concerned about the representations that are made to consumers and that they might see on their individual devices. And the fact that those representations and those practices involve sensitive health information is another factor that we consider and would definitely make us examine representations made in a very serious light.

MS. PRITTS: Okay, so, I have a follow-up question on that, which is: Does the FTC have a vehicle online for consumers to report apps that have privacy and security issues?

MS. HAN: We do. So, if you go to the FTC's Web site, we have a consumer complaint hotline and you, I believe, can call or submit complaints to us and we also have a large database where we track consumer

complaints called Consumer Sentinel, and that allows us to determine if a particular company has had a lot of complaints lodged against them and other sorts of trends.

MS. PRITTS: So, Sue, OCR similarly has a number of ways that are posted on your Web site for consumers to file complaints about what may be privacy and security violations, including those involving mobile applications, right?

MS. McANDREW: Yes, we do have complaint forms that are available through our web site and that can be submitted, downloaded and e-mailed back to us, or submitted through the mail.

MS. PRITTS: Okay, and I will ask the FCC and the FDA if you have similar consumer-facing parts of your web site where people can file complaints if they feel that it's necessary.

MR. PATEL: Absolutely. From the patient safety part, we have for all medical devices or anything related in the use of medical devices, patients, users, clinicians, caregivers can submit anonymously complaints

or event notifications to us that we can follow-up later on and come up with the same kind of analysis like FTC does. Is it happening in particular area? Is it happening in a particular situation? Is it happening in a particular device? And then we follow-up with that. So, we do have -- and it's all on FDA's web site. It's called MedWatch, if that rings a bell. They should probably look it up.

MS. PRITTS: Okay, thank you.

And, Geraldine?

MS. MATISE: The FCC does, as well.

MS. PRITTS: Okay. So, there is for those of you who are interested in reading more about all of these different federal efforts, there are links that are posted on this event's web site, which will readily get you to some of the proper places that we've talked about today.

So, I think what we've managed to do here is give you a little bit of an oversight of what at least the framework is that we're going to be looking at in looking at mobile devices. As we said when we started,

that this isn't happening in a vacuum. There's a lot of regulatory protection and guidance already out there, and what we're looking to do here is to make sure that as people are adopting these, that they're aware of these different requirements and that they have very practical ways of addressing them.

So, I'd like to get you in join me in thanking our panel. They've been wonderful in helping us understand this very complicated and overlapping jurisdictional issue. Thank you. (Applause)

We're going to have just a very short break here while we reset the table for our next panel, which will be Real World Usages of Mobile Devices by Providers and Other Health Care Delivery Professionals.

(Recess)

MS. PRITTS: (Inaudible) for our panel here. We're getting ready to seat our next panel, so, we'd like it quiet in the audience, please. Hello, quiet. Thank you.

All right, our next panel, which is going to focus on Real World Usages of Mobile Devices is going to

be led by Dr. Jon White from the Agency of Health Care Research and Quality, fondly known by people inside the beltway as AHRQ.

Dr. White directs a health information technology portfolio at AHRQ. He sets a programmatic direction of AHRQ's health IT projects. We do a lot of work with Jon White and his team, and I tell you they are just a pleasure to work with. They have fueled and informed a tremendous expansion of health IT to improve health care quality, which is what it's really all about. So, I would like you to join us in welcoming Jon and the members of the second panel to start this discussion of how these devices are really used in real life. Thank you.

Welcome, Jon.

DR. WHITE: Well, thank you so much. I appreciate you all being here today. Welcome. I want to welcome all of our friends out on the Internet, including potentially my family. Hi. Who are going to be watching us today and listening to a really engaging conversation. So, we've got a great panel lined up for

you. I'm not going stand long in their way.

Today, we're talking about the intersection of policy and technology in great health care, and there are a lot of those different intersections, but in particular, we're talking about mobile devices. So, yeah, we talk about the devices, we talk about the policy, but what you're going to hear, I think, from these folks today are really that we're talking about putting information in the hands of people who need it to be able to deliver better health care. So, it's not just the device and it's not just the information, but really it's the power to transform the care that you deliver and to be able to do the best job that you can when you're trying to provide that care. So, like I said, we've got a great group of panelists. I'm going to let each one of them introduce themselves individually. They're going to have a chance to talk about where they're from and what they do and really the most important thing that they've noticed in terms of mobile devices and the relationship to the care they deliver. And then we'll get into some great discussion.

So, please.

DR. DeLaROSA: Good morning. My name is Jacob DeLaRosa. I am from Pocatello, Idaho, and Idaho does exist. (Laughter) I'm a practicing heart surgeon and clinical work, 90 percent fully clinical. It's a passion in myself in regards to mobile devices. I came up with an app about three years ago in regards of protecting people from texting and driving because there's just been so many accidents that we had seen. So, it's sort of a passion in regards to mobile devices.

But, as well, the mobile device in regards to medicine and really in clinical practice is essential and I was sharing this a little earlier, how imperative it is when talking to patients and actually showing them the disease process, showing them the complications, showing them what's going on so they could see it one-on-one versus just an explanation. And it's still very shocking to me that I'm fourth down the line before I see a patient for open-heart surgery, for cancer surgery, et cetera, and the patient has never seen what they're being treated for because it was never shared

with them. So, for me, it's really important about the awareness of the technology we do have to share with physicians and then they learn what's available.

MS. GALLAGHER: Good morning, everyone. My name is Lisa Gallagher, I'm Senior Director of Privacy and Security at HIMSS, the Health Information Management System Society. HIMSS is a cause-based, not-for-profit organization that's focused on the optimal use of IT for the betterment of health care. We have 44,000 individual members, 570 corporate members, and 170 not-for-profit organizations that participate with us and share our mission.

The reason that I'm here today is because HIMSS has a number of initiatives that are related to the use of mobile devices and health care. First, we have an initiative called mHIMSS, which is focused on building on HIMSS' already existing strengths and convening stakeholders, sharing knowledge, providing education, public policy, research, and content, and here, our initiative is focused entirely on mobile technologies that are used in the workflow and for data

exchange, and under the mHIMMS's initiative, under the direction of my colleague in the back here, Edna Boone, we have two interesting efforts that I wanted to highlight and I'll be sharing some data from these as we go throughout the discussion.

First of all, this past fall, we executed our first annual mHIMSS Mobile Technology Survey, and that was related to the use of mobile and wireless in health care organizations, and they're used for access to patient data, how folks are attempting to secure data at this point, and the benefits and barriers of the use of those technologies. So, I'll have some data to provide as we go through the discussion. We also have an upcoming conference, the mHealth Summit in December in Washington, D.C., and then in my area, in the privacy and security area, we had convened a mobile security workgroup this year and they recently published a mobile security toolkit and that has various reference resources, best practices, case studies, et cetera, and as we go throughout the discussion, I'll also talk about some of those work products, some examples that we have

that are useful for today's discussion.

And I think to Jon's point as to what are some important points that I want to stress at this point are that we do see from our survey and our data that we collect that one of the most prevalent issues that we're seeing, especially with regard to privacy and security, is that the technologies are being deployed in health care organizations without the benefit of having updated policies and procedures in place for managing them, and, so, that's some of the information that we have in the toolkit and then I will talk a little bit more about some of the concerns and benefits, but, of course, privacy and security does come to the top.

DR. WHITE: Thank you very much.

DR. HEILMAN: Good morning. My name is Steve Heilman. I'm the chief medical information officer for Norton Health Care. I am an emergency medicine physician by training. I've been doing the CMIO work for the last three years and I'm sort of learning on the fly as I go, but part of my job is to help oversee our organization.

Norton Health Care is located in Louisville, Kentucky, where an integrated delivery network of five hospitals that are not-for-profit, including a freestanding pediatric facility. We have 15 outpatient centers, we employ about 12,000 employees, we have 2,000 physicians on our medical staff, 500 employee physicians on our staff. We have about $1.5 billion yearly in revenue. We have about 1.5 million patient encounters annually, 60,000 admissions, and we're really trying to get our handle on mobile technology and what we could bring to the table.

One of the things, I guess the key salient point I'm trying to make, in my job is that mobile technology is developing very rapidly and we're seeing mobile devices show up more and more frequently, multiple types are coming to the table, and we ourselves have sort of a bring your own device policy that we're trying to develop, as well, as to giving our executives and administrators our own devices that we know we can control. The problem is, as mobile technology expands so rapidly, back to Lisa's point, we're still trying to

figure out how can we govern that and we're finding out that if you don't have policies in place to help govern that, it becomes sort of the wild, wild west out there in health care. I think benefit and communication is absolutely paramount to helping take care of patients and communication between providers, communication between patients is excellent. It helps decrease length of stay, it helps gets feedback, it helps improve care.

The problem is we're finding that clinicians are taking advantage of unencrypted video conferencing on the Internet to kind of do patient handoffs; we're finding that nurses are texting physicians with patient's personal health information. So, even though we're trying to figure out what polices to put in place and how to govern them while all this is going on, you have to get in front of that because if you don't have those policies in place and educate everyone about what the risks are of that, it will just go out and not be controlled. So, that's really what we're trying to get ahead of right now.

MS. SHAFFER: Good morning. My name is Meri

Shaffer, I'm an RN, and I'm currently working as a systems analyst for Montefiore Home Care. I have over 30 years of homecare experience, and for the past 15 years, have implemented and worked with various technologies that allow for better patient care and clinician efficiency in the homecare arena.

Montefiore Home Care is celebrating 65 years of service to the communities of the Bronx and Westchester Counties in New York. We are part of Montefiore Health System and are the first hospital-based homecare agency in the United States. We are large, with a census of roughly 2,200 patients combined from our certified agency and long-term Lombardi Program.

Homecare in both urban and rural settings each have their own challenges, but, at the same time, we still have a lot in common. Lengthy documentations requirements for compliance and billing, patients that are coming home sicker with multiple chronic illnesses, gas prices, and reduced reimbursement are issues all homecare agencies face. The use of mobile

technology to assist the clinician in rendering quality care to the patient is now becoming the norm. Safeguarding that health information becomes an important matter.

Currently, many agencies, including Montefiore, go ahead and furnish devices to clinicians for use for documentation purposes. One reason for this is we can control the security. Currently, we use laptops with touchscreens. These laptops not only have encrypted software from our vendor, but we are also encrypting the disk, as well. Other agencies I know of also use LoJack Software in case the laptop is stolen or lost so it can be recovered. Licensing surveyors recently are now asking for policies about security and agencies are really scrambling to comply and they need guidance.

There is also concern about the use of public Wi-Fi and cellular technology. Texting is really convenient, but is it secure? No. Some of the agencies have policy about texting and, but, again, these are really difficult to enforce. Some of them

just use patient numbers or initials, but it doesn't seem to be a workable system.

Also, there's a concern about clinicians using public Wi-Fi. Is that really secure? There are some colleagues that I have in the rural areas where difficulties of available high-speed Internet and cellular coverage is an issue, and, believe it or not, even in New York, cellular coverage can be very erratic.

And none of this is without cost. Homecare is, unfortunately, not included in the American Recovery and Reinvestment Act Incentive Program. So, we have to pay for all this ourselves. Despite the challenges of utilizing mobile devices though, the main payoff for clinicians in the field is having accurate information when seeing patients. The ability to gauge improvement or decline by comparing the patient status from visit to visit allows for clinicians to note whether treatment plans are working, communicate aspects of the patient's condition effectively to the physician, and enable the

physician to make better care decisions for the patients.

I want to thank the ONC for inviting me to give input on this subject that is very relevant to homecare. Thank you.

DR. TASHJIAN: Good morning. Hi, I'm Chris Tashjian. I bring a little different perspective. I practice in a town of 1,500. I'm kind of the classic family doc. I see patients in the hospital, I work the emergency room, I see patients in the outpatient setting, and I also do nursing home, and, believe it or not, even occasionally see the county jail patients, as well. So, it's kind of a little bit of everything and my passion, of course, is health care and medicine and caring for my patients, but a second passion is technology and mixing these passions and finding out how in using technology to really improve the care of my patients and demonstrably show that we can provide world-class care in a setting of 1,500, in a town of 1,500.

I think technology is a great equalizer. I

think the next step in that is going to be the mobile technology, but if we look back for a minute, I mean, I've been using a smartphone for 10 years and it's really interesting because 10 years ago, we were using it just as access to medical information, and even then, if I looked something up in a book my patient said, what's the matter he doesn't know anything? But if I pull out my palm and look it up on an Epocrates, they say man, this guy's really smart. Look at how he can use the technology. (Laughter) So, again, technology, I think, has been here, but it is just now mushrooming and even in the rural areas, we welcome it.

I look forward to it for doing a couple of different things. One is interactions with specialists, as you can expect, when you're in the rural setting, you don't have access to specialty care, and, so, technology can be the great equalizer in that aspect, but I also look at it in how can we better serve our patients? And, for example, and I've asked numerous patients this, if I could text you your results, if I could give you information via your mobile phone, would that be helpful

to you? Would you rather receive it in e-mail, would you rather receive it in snail mail, and 100 percent of the time, and a few things in medicine that are 100 percent, but 100 percent of the time, they say if you could text it to me, that would be great. If I would have to do less, could just get that data as soon as it's available, and to be honest with you, they're expecting it and I think we need to give it to them.

Finally, I'm going to close with one thing that I think is really interesting, is I share a picture with people that is of my 90-year-old mother and my 89-year-old mother-in-law and on Christmas Day, they are sitting at the kitchen table with their iPads and they're beating on their iPads, and, so, I don't think this is a generational thing. I think the vendors and the people like Apple have made the interface so easy that virtually anybody can use it. I think it's now incumbent on us in health care and in the health care vendors to find a way to get it to them because I think it's possible and I think we have an obligation to our patients to do that. Thanks.

DR. WHITE: All right, what a great introduction. So, I hope it is clear to you these are not nerds with stethoscopes. (Laughter) These are people on the frontline of health care delivering care and working with their colleagues to deliver care using powerful information tools, and that's what we want to hear and that's what we want to do, and they also have an appreciation for the issues that go along with that.

We're going to launch into a discussion of a couple of different questions. We're going to take questions from the audience, from Twitter, and from the Internet. I do want to take a brief moment to thank my colleagues from the Office of the National Coordinator, Joy, and her colleagues. Not only are you all charming to work with, but really talented and smart and you set up a great panel. So, I appreciate all the effort that's gone into it today. So, thank you very much.

So, let's start into it. You guys mentioned a couple of these, but I really want you to talk a little bit about the kinds of things that health care providers do with these mobile devices. We're drawn to

them and there are certain things that we do and there's the things that really make a difference, right, and say wow, I couldn't do that before, I want to hear about this. I also want you to talk about the things that you want to be able to do with it, and it's not quite there yet, but you know that if it could just do this or that, that really you know that it's going to make a big difference for you. So, what are you all seeing?

DR. DeLaROSA: What I use it for, I use it primarily for CAT Scans, radiology-type of procedures that I can get and get them pretty quickly. The delay is the download, especially on these multi-sliced CT scans. We also are able to see in live is a coronary angiography. So, it's sort of like your office has become mobile. So, now you don't have to be sitting in the hospital and be getting a phone call from cardiologists, a radiologist, a referring doctor, and he says can you look at a patient's films? Yes, and I'm able to now look at the films using a mobile device and now being able to give my opinion right away. And this goes back to the rural physician, too, that calls and

needs help with something. You can now look at these films and make a decision right away versus trying to drive to the hospital or trying to get someplace through traffic to give an answer. So, that's what I use it for mostly.

What I would like to see, I would like to see things faster, of course, and if being able to do sort of like a face time with the physician you're talking to because one of the things that I think we sort of lose is that personal touch of you can be talking with somebody or you can go without seeing them, seeing facial expressions and seeing and understanding back and forth.

DR. WHITE: Radiology is always in the basement, right? So, you no longer have to run from seven down to the basement and then back up again to see your film. So, great point.

DR. TASHJIAN: Yes, I was going to say a perfect example, and Dr. DeLaRosa kind of touched on it, but it's interesting, a year ago, when I'm in the emergency room and somebody comes in with a complex

fracture, and I'll be honest, I'm not an orthopedic surgeon, but I need one, but I need to know how to explain it to them. At least at that time, willingly or unknowingly, we would text them a picture of that x-ray and they would be much happier than anything I could do, than anything I could explain over the phone and they could tell me right then and there admit the patient, don't admit the patient, splint the patient, I'll be in right away to take care of it. Any of those things.

We've had to stop doing that because the HIPAA people at the hospital said you can't do that. We're working on work-arounds and one of my goals is to not have to do work-arounds, but design it right from the ground up. One of the work-arounds that we're at least going to look at is what if we just take a picture of the fracture, but no patient identifiable data? So, we can do that, but my goal is to really look at it from the ground up and ask the vendors make something that we can use.

DR. WHITE: So, that's a great policy issue, right? So, and you call them the "HIPAA people," and I

know, right, that's what we all call them. They do have responsibilities and they --

DR. TASHJIAN: I'm not saying it's wrong.

DR. WHITE: Love the HIPAA people.

DR. TASHJIAN: And, again, as a patient myself, I don't want my data out there for anybody to see. So, I understand where they're coming from.

DR. WHITE: Yes.

DR. TASHJIAN: But I also understand technology can do a lot of things and technology, at least to me, it's coming under vendors to give us technology that satisfies the patient privacy and that I want both, I want privacy and I want to be able to use it.

DR. HEILMAN: So, we have academic affiliations with the University of Louisville and the University of Kentucky, and one of the most prominent apps that was first taken advantage of and we've been doing it for probably 5 or 6 years is just the online education, much like Epocrates or a third-party resource just for drug dosing, drug interaction, best evidence-

based practice medicine. Generally, on those applications, we get between 4,000 and 5,000 hits a month. So, those are very active and very prominently used by our medical staff.

Additionally, technology is getting to expand greater, and, so, we're starting to see the ability to transmit fetal monitoring to smartphones and smart devices. So, our OBs are extremely happy with us right now because when they're on call, their nurse has a question, they can actually just pull out their phone, go look at a fetal tracing, and say no, that's normal or no, this is of concern.

Technology is expanding. We're now even monitoring in ICUs those monitor readouts and rhythm strips can be put on a smartphone for patients to see. That's a huge advance. So, if you're monitoring multiple ICUs or you're on call, physicians find great value in being able to get to that data and that information really quickly.

Those are probably the biggest things we're starting to see. I think it'll be great as telemedicine

evolves, to what Jacob talked about, getting that face-to-face interaction to be able to talk with your patients and see your patients in a secure environment and actually provide care that way. I think it'll really take medicine to the next level.

MS. SHAFFER: In the homecare arena, I think that since we see patients in the home, one of our great challenges is medication reconciliation and the fact that we have very disparate systems out there. So, to have an accurate medication list that we can confer with the physician on so that we both are on the same page, we have a really greater chance of keeping people at home and not having them readmitted to the hospital. So, I think disparate systems is really a big challenge.

MS. GALLAGHER: So, just to give you some sampling of the data that we collected on the work-related tasks that providers are using mobile devices for, the top use of a mobile device is to look up non-PHI-related health information. So, information that guides the provider in providing care. But the next one is 75 percent of the respondents used the mobile device

to view patient information. Twenty-eight percent actually report storing that information on that device, but seventy-five percent use it to view. They use it for education and training purposes, clinician notifications, tracking of work lists, so, their tasks during the day, and 33 percent report at this point in time using it to provide secure communications to their patients. There are some other smaller usages, collecting data at the bedside, analysis of patient data. So, viewing, but then doing some analysis-related task, et cetera.

With regard to some of the challenges and concern areas, in my introduction, I talked about the fact that privacy and security is a top concern, but, actually, looking at the data here, the top concern among all respondents was actually the speed of accessing the data. So, now that they found ways that they can use these tools to review clinical information or images, the actual download speed is a concern, as well as screen resolution and fidelity. So, as we start to use these tools in the clinical setting as part of

the clinical workflow, there will be some technical challenges to address, as well.

DR. WHITE: Since a lot you mentioned the speed, I'll just briefly mention that there's the pushing of actual information to the device. Increasingly with the cloud coming to be and we're seeing the push of not whatever it is, the file, but the image of processing that's being done at a different place. So, there's hope for that, but I totally agree with you all.

You all come from a wide variety of different types of practices and where those practices are located. Anything special about the environment in which you practice or your colleagues practice that speaks to you about how these devices are being used or they want to be used or how they make a difference?

DR. HEILMAN: So, we have about a 50-50 mix between specialists and primary care and we're just in the deployment phase of our new electronic medical record, but one of the things that comes with that is an application for the physicians to use that's a native

app that sits on their smartphones essentially, and that one of the benefits we're realizing quickly is that the primary care doctors who cover for other physicians when they're on are able to access those medical records, and that's predominately in a read-only format, so, there's some challenges in what you can do with it, but if someone does call and it's a complaint that you can go back and access the record, look at the medication list, look at previous histories, see if they've had these problems in the past, it does enable them to really provide much better care than just kind of going on the fly and trying to resolve the issue by just the data that the patient is giving them.

So, I think that access has really leveraged them to be more productive. Additionally, it does allow them to do prescriptions through their phone, as well, and I think they're finding a lot of value in being able to just file a prescription quickly through the smartphone application, as well.

DR. TASHJIAN: I will echo what Dr. Heilman said, but what we're finding is that, again, access to

information and data is crucial, is that being able to look up the record from virtually anywhere is great. We're seeing though a lot less ability to actually do something or act on the information. So, either writing a prescription, sending an order to the hospital, or doing something like that. So, we're actively working with at least a couple of vendors to say we need to do this, this is really important.

DR. WHITE: So, not just getting the information, but being able to act on it --

DR. TASHJIAN: Exactly.

DR. WHITE: And do what clinicians do, right? Okay, cool.

Steve mentioned this. If anybody wants to comment on it, bring your own device versus enterprise-owned. There's issues on both sides. Any thoughts on how you address that or how you go about making those decisions?

MS. SHAFFER: Well, I know for us, it was really a security issue across the board. And most of our clinicians are nurses, physical therapists,

occupational therapists, they're not apt to bring their own device and buy into that. I think they're expecting to get a device. And, plus, for us for supporting it and for security issues, it's much cleaner. Much cleaner.

MS. GALLAGHER: So, in my area of privacy and security at HIMSS, the number one question I get on the use of mobile devices is: If we decide to allow individuals to use their own device, how do we manage that? So, in our toolkit, we've provided a number of reference resources on how to manage that and up to and including once you've decided to allow the employees to bring their own device and connect it to the network, what would a sample user agreement be so that the end-user is educated about what are the implications and what are their responsibilities when it comes to the use of those devices to access the network and to access patient data?

So, I do have a sample mobile device user agreement in the toolkit and those samples, policies, and user agreements are provided by our members who have

actually implemented them and are in their organizations and find that they're working well for them. So, I think this is a trend. The advantages, of course, are the ability for the end-user to use his own device for multiple purposes, both business and personal, but also organizations are finding that it saves them a tremendous amount in the cost because they don't pay for the device and they don't always pay for the access. So, it reduces expenses, as well. So, it is realistic, it is being done by lots of organizations, and, so, we've got to really get a handle on the policies and the training, education, and agreements that the end-user or the employee needs to understand.

DR. HEILMAN: If you took a snapshot five years ago and you called our help desk, we only supported Blackberrys and PCs, and if you asked a question about an iPhone or a Mac, we told you we don't do that. And we were able to stick to that line for a good year until the outrage got much too loud for us to be able to manage. (Laughter) And, so, we had to kind of open it up. And I think it's the right choice.

The problem, as Lisa mentioned, is that when you do this mixture and you're saying it's great to bring in your own device because we can never afford to provide 12,000 employees each with their own mobile device and pay for those contracts. They need to understand what risks are going on. If you're going to use our network, then if you have multiple incorrect log-ins, we're going to wipe your phone. If you're going to do this, we're going to have the ability to locate where the phone is if it gets lost or stolen. Those are things that some people are comfortable with and understand. It's the benefit of being on the network, but other people have taken real issue with that. And, so, it's a mixture. We're finding some physicians are willing to do that because they feel it eases their job, but others are saying I feel that's too much like big brother at this point and I'm not ready to commit to that.

DR. TASHJIAN: I take a little different viewpoint, and, again, I told you technology is, again, one of my passions. I find that I don't want any of

that information on my phone. I want to be able to access it, I want to be able to see it, but I don't want anything to do with storing it, and I think that that's out there. We specifically chose our EHR vendor because they could give it to us in this ASP format, which is essentially saying that our data is in the cloud or it's in Kansas City, even though I practice in Wisconsin, and that's been a lifesaver for us because we don't worry about security, we give that to the technology people and say that's your problem. My problem is taking care of the patient. So, anything we do mobile-y, my request to the vendors is I don't want it on my phone. A, I don't want to store it, and, B, I don't want to be responsible for it.

DR. WHITE: I think most of us may have, not that I've done this, dropped their phone in the toilet at one point and lost something that was important on it. So, you can appreciate the value of doing that.

So, I'm going to ask you one more question and we've got some great questions from the audience and from online. So, you were talking about the power to do

things that you couldn't do before when you didn't have this information with you, which is great. With great power comes great responsibility and we're talking about privacy and security here today. So, are you or your colleagues aware or do you talk about the privacy and security issues because you just started to touch on this. That's your problem. To what degree are these things discussed by us as health care providers or is it just I just need the information I need?

DR. DeLaROSA: This has gone up to already the Ethics Committees because it does become ethical when you're carrying people's data around, patients' information, and what do you do? And the way that we've been able to sort of solve it in a low-cost manner is you have to commit to it, you have to sign a contract, and you have to have your phone guarded, meaning you have to have a passcode on it. A lot of phones don't have passcodes, but if you're going to commit to carrying patients' information on it, then you have to have a passcode. So, when it does get lost, if you do leave it on the airplane, if you do leave it someplace,

it cannot get into, and that's the way we've been kind of been able to deal with it at a lower expense level.

MS. SHAFFER: In homecare, I think it's a topic that comes up all the time. It's covered heavily during orientation and on a yearly basis. All clinicians, I know, at our agency are quizzed on HIPAA rules and regulations. So, it's definitely in the forefront.

DR. TASHJIAN: Yes, I would just echo that even in our small town, it was a week ago that every single person, including our medical assistants and everyone, and, again, we basically have to undergo training on HIPAA, which, again, we think is a good thing. I will say this though, I think paper is much more likely to be lost than electronic data and I think we can't lose sight of that. I think that we kind of sometimes forget when we leave a briefcase here or we leave something there that paper is probably less encrypted, more easily lost than the electronic data. So, we think of this as an improvement.

DR. WHITE: Very good. Okay.

Okay, yes?

MS. GALLAGHER: Okay, so, I know that we're talking about this from the provider or physician perspective, but there are some very serious security concerns for the IT folks, the network folks in that when you allow these kinds of devices on your network wirelessly, you're dealing with almost an uncontrolled number of remote accesses and I know that with the HIPAA audits, remote access is an area that HHS is asking everyone to focus on and they have actually issued a guidance document which I think is on the OCR site on the security risks of remote access. So, I think it's a security risk management issue for the IT folks.

I also want to mention that we are seeing a trend towards wireless medical devices, monitoring devices, et cetera, and those are also connected onto the network. Those are most often managed by the clinical engineering biotechnology side of the house and at HIMSS, we have an initiative, a clinical engineering IT community where we're trying to get the IT folks and the clinical engineers to talk to each other about the

devices that are on the network. Both sides need to understand that it is a remote access, but you also have it connected to a live patient.

It is a security risk management issue from a number of perspectives: integrity, availability, et cetera, but also you have the IT folks doing security network monitoring, perhaps vulnerability or penetration testing and not realizing where the medical devices are on the network and connected to live patients. So, that's an area where we think there needs to be a little bit of work and communication. But, that having been said, there are lots of tools out there for you to use, guidance from NIST, guidance from HHS, information in our toolkit, et cetera.

DR. WHITE: Great. Okay, so, let's start with some questions from the folks out here. We'll start with Steve, a question for you, but then we'll open it up to other folks, but give you the first chance to answer. Can you discuss the role of mobile devices and transitions between care settings?

DR. HEILMAN: Well, from an inpatient

perspective, I think it does take a good role because then nurses can do handoffs, essentially send information in a secure form so that they're more informed. We're used to the days where I'm going to fax the report to you and if we can get away from faxing, that's great because we can keep things not on paper and not lose things that are moving around. So, I think there's a huge thing and huge capability with that.

We don't do home health, but I do see a large value in transitioning patients from an inpatient or acute care setting to a long-term care. I think that's something we're going to have to work on in the future, but I do think there's great value in being able to leverage mobile technology to get that accomplished and I think that probably dives right into you, yes.

MS. SHAFFER: Absolutely. I mean, I think that link between the hospital and the homecare or even the nursing home for long-term setting is essential and to get up-to-the-minute information so that what we bring in the house is actually what's needed, I think, is essential.

DR. WHITE: Okay, I'll go with potentially leading question. Would you agree that just having a policy for privacy and security does not mean compliance and that a simple way to monitor compliance would be valuable? Discuss. (Laughter)

DR. TASHJIAN: I think all of us would agree with that, I think that's a pretty straightforward question. And, again, I look for ways, and I'll say it again, I look for ways that make the technology do the work. I want it to work for me. So, I want the technology to make it easy to monitor or to make it so that you don't have to monitor. As I said, if the data is there to view but it's never stored, it makes monitoring much more simple.

MS. SHAFFER: And I think coming from different facets of homecare, you've got hospital-based homecare that has great IT support, they've got huge IT departments, and then you've got these small agencies that I've met in the past where they have very little guidance or they're subcontracting out IT and these people may not have or very limited knowledge of HIPAA

and what's required. So, I think some standardization would be really helpful in the long run.

DR. DeLaROSA: I'm going to touch on the IT perspective because I think that it's very important. I mean, IT is a support staff of a hospital and this outsourcing of IT is, I mean, it's not that it's good, it's not that it's bad, but in my own situation, I see the limitations of as we're trying to employ EMR, in terms of all of these new devices, everything moving forward, and there's not enough support to be able to support the physicians and teaching them how to use the mobile devices, the electronic records, et cetera, as we're moving forward.

So, I think one take-home message that I would state is that really IT is essential in moving forward with what we want to do because it's just not there and not all hospitals and all organizations and we do find this outsourcing happening more and more and it's very difficult when you have a problem as a physician that all of a sudden you get put on hold and it's in Plano, Texas, or it's in New York City, and then

somebody will get back to you in 24 to 48 hours. So, something to consider that IT is essential in moving forward with this.

DR. WHITE: From what I've heard, as well, it's a real issue for providers in places that they don't necessarily have access to folks who are trained or capable and getting workforce across the country where health care is delivered that can provide you that kind of support is really important and critical and successful use, whether it's mobile or other kinds of IT. For what it's worth at AHRQ, we've heard that a fair amount.

So, Lisa?

MS. GALLAGHER: So, the question was whether we believed that simply having a policy is enough for compliance. So, as we all probably know, the compliance regime that we're dealing with is primarily risk-based. So, whether it's HIPAA or whether it's meaningful use requirement or measures, we're talking about doing ongoing security risk management. Oftentimes, if organizations are doing security risk analysis at all,

they're just doing it once and they're documenting it and moving on. So, really, the connection between the policy and procedures, what employees are supposed to be doing as part of their use and access to the data and what they're actually doing is the connection that we need to make. So, training them, having them understand the policy that does exist and that is important and the procedures that they need to follow, but also monitoring somehow what they're actually doing, what their actual practices are in trying to manage that and getting them back in compliance with the procedures is really the scope of the full risk management process. And, so, you don't just have a policy that's on the shelf; it's used as a tool for employees to understand what they need to do as part of their workflow.

DR. WHITE: Okay. So, you all have grappled with these issues extensively. I'm not going to ask you to necessarily tell personal stories, but if you were confronted with the situation, right, where something happened, right? Somebody left a phone somewhere or whatever and information got out, how do you think that

would affect, A, the way you're using it or the way your colleagues are using it, OK, at the present time and then what do you think would happen to move forward? Everybody has kind of that sentinel moment where ooh, that happened. Maybe it's happened to you, maybe it hasn't, but if it did happen to you, what would happen? Did everybody suddenly go oh, my God, we weren't thinking about that or yes, we were thinking about that, but one slipped through. Can you relay any experiences like that, without naming names, of course?

MS. SHAFFER: I think it brings a definite heightened awareness of protecting the device itself because we've had a laptop stolen and it's a scary prospect and I think we go ahead and we share that and we make sure that the staff is aware of it that you can't leave it in the trunk of the car, you can't do that. People will break into your trunk and take it. So, I think it brings a heightened awareness and I think a new certainty about what they're supposed to be doing and not slacking and not following the policies that we provide.

DR. HEILMAN: Those set of events usually bring a rapid cease and desist order from our Compliance Department, and then broad-based education and the new policy and then education more and then more enforcement. So, I mean, that's just sort of the route things take coming down the channel.

DR. WHITE: So, that's like within a big infrastructure. Chris, if you're not a big infrastructure, what does do to you?

DR. TASHJIAN: Yes, again, and I think it goes back to let's let the technology do the work. So, anybody who has -- we don't use laptops, but we use tablets and we use mobile phones, and they can all be remotely wiped. So, the real question is: As soon as you find out that you've missed it, it's incumbent on you to first wipe it and then tell us.

DR. WHITE: Night-night, iPhone. Gone.

DR. TASHJIAN: Yes, and just render it useless, and it's really interesting because I don't know how many people are aware of this, but every iPad has a unique number. Every iPad can be wiped from

access to the Web from any spot in America or any spot in the world, really.

DR. WHITE: Yes.

DR. TASHJIAN: So, again, is take advantage of the technology and then we do stuff. As I said, in homecare, you need laptops. We don't, and, so, we take advantage of that because I don't know how to remotely wipe the laptop that's not plugged in.

DR. WHITE: Jacob?

DR. DeLaROSA: Well, it's about education, but an example in a smaller arena is in the operating rooms. And when you're operating, the physician leaves their mobile phone to be answered by a nurse, circulator, or somebody in the operating room. And an incident that happened was a risqué message came through on a mobile device.

DR. WHITE: Nice.

DR. DeLaROSA: Which then was accessed by whoever answered it and it was supposed to be a personal message. And that brought out a lot of education because that happens. (Laughter)

DR. WHITE: AT&T moment, right?

DR. DeLaROSA: Yes, it was a moment. Yes, it was a MasterCard moment. It was priceless. But it was, right away, the education came back about that you're not the only one seeing these sometimes and now save the private information. I mean, it could have been about a patient, but it was, again, another personal message. So, right away, that became an education, everyone had to go through education. Physicians, nurses, techs, et cetera, so, that's how it gets around.

MS. GALLAGHER: So, six or seven years ago, when I was still doing consulting, I was working in a small hospital doing a risk assessment, and I asked the IT guy, I said, what do you do if a physician loses two or three mobile devices in a year, because it had happened at that hospital, and he said well, we give them another one. (Laughter) So, and I said well there's no consequences? Oh, no. We have been told we don't, we can't do that. That's six or seven years ago. Now, I think there really is an awareness and it's brought about by a number of things, not the least of

which is the breach notification process and the wall of shame that's maintained on the HHS web site. I get calls all the time about that. Look, the organization's name is on there. There is a much broader awareness and I think it goes all the way down to the individual employee level that the physical protection of mobile devices is very, very important. It's then how do we implement that and how do we monitor that, but big difference in the last few years.

DR. WHITE: Okay, we've asked the Internet, and the Internet has responded. So, we're going to go with a couple rapid fire questions here. So, I like this one. How does a provider know if they're buying or using a trustworthy app? That's like *Monty Python*. How do you know she's a witch? (Laughter)

DR. DeLaROSA: Yes, I mean, that is challenging and you go by reviews. You try to see other people's reviews to see if it is a legitimate app, if it does work. From a personal experience, I thought I was downloading an app that somebody had told me about for calculating BMI, Body Mass Index, and BSA, and I did and

the next thing I knew, I was sending messages about Viagra and Cialis to everybody from my account. So, I got --

DR. WHITE: Oh, Dr. DeLaRosa says so.

(Laughter)

DR. DeLaROSA: Yes, so, I mean, I got some kind of Trojan Virus or something on there then I had to get it cleaned off and get a new computer, actually. So, again, you don't know, you try the best you can, you go to reviews and see what people say, but it does happen.

MS. GALLAGHER: So, my advice would be assume that it's not secure and the apps that are used in the clinical workflow should really be vetted by the organization and everyone should receive training on them and understand the security controls that are contained within that app, and if that's not the case, individuals should not be downloading apps for their own usage in the organizational workflow.

DR. WHITE: All right. Let me jump to the next question real quick. I want Dr. iPad and iPhone

and the smartphone for 10 years to answer this. What are your top three considerations for apps and what design feature do you look for?

DR. TASHJIAN: Well, what we've talked about, what we've used for the 10 years is I want access to information. So, information like Hippocrates up-to-date, something that can help me right here and now when I need it.

Second thing I want from it is access to my records or access to the patient records. I mean, let's be honest, they're not mine, they're the patients', and I want access to them so I can provide better care.

And the third thing I want is a way to communicate with my patients, and I'm not sure if that's not the first one, to be honest with you, is I want to be able to use that device to send information to my patients, i.e., your cholesterol is this, let's try something and come back and see me in two months or how's your child doing? I knew he had a fever yesterday; can you just touch base with me and let me know that they're doing okay? That goes a long way to

care, that goes a long way to reducing the cost of care, and it provides a better experience both for the patient, but also for the physician.

DR. WHITE: Yes, my family's practice has been wired for a couple of years, but I'll tell you, the biggest difference it makes is being able to say oh, I got this quick one, zip it off, and my provider is outstanding within an hour or two, zip, he answers right back. I'm like oh, good, I didn't have to worry about that falling off my plate, I don't have to worry about not having the answer for a long period of time, so, I'm with you on number one.

DR. TASHJIAN: Let me give you an example of that because, just yesterday, I got a call from somebody who says I know I have testicular cancer, doc, I know I do. He gave it to me and he was so worried and he was so concerned, but having the ability to schedule an ultrasound and get it done and tell him relax, this is going to be okay and do all of that within a period of five minutes is tremendous. Now, some people say yes, but aren't they bothering you? I said it doesn't matter

what happens. If he does it in the old-fashioned way, he calls the office and my office calls me and then I have to tell my office to do this, it actually takes me more time. So, in a lot of ways, it saves time.

DR. WHITE: Yes.

DR. DeLaROSA: I just want, a caution to providers, that we can't just be so cavalier and we cannot forget in regards to the one-on-one and the personal experience. I sit on several committees, and one of them has been just sending messages that you have cancer or the test was positive. Those are not the things that you want to send by text, by e-mail, and I'll see you on Monday. Those are the things that are still communicated one-on-one. It could be over a telephone, but it has to be still communicated, and I think I have to caution providers that we're getting to this, again, this grey realm, being able to communicate right away, but, again, let's not forget what messages we're sending at the same time.

DR. WHITE: That is an outstanding point. I appreciate you bringing it up.

In the same vein, but with a slightly different take, this is a good question. In the course of your interactions with patients, have those patients expressed concern regarding the security of their personal health information? Do they ever freak out when you pull out your device and go oh, you can do what, where?

DR. HEILMAN: You're going to get a mixed response. I mean, there are some people that do that, there are some people that don't. I mean, our patient portal, the average age of the person who accesses that -- or their information is getting online right now is 69. Our oldest person is 82, I think. So, I mean, and we're just rolling it out, but my point was that it's not necessarily age differential about people who are concerned about their information being out there. I think a lot of people know technology is coming, they're impressed by the technology, and if I could walk in an exam room and show them their fracture on my iPad or show them that CT scan, they're impressed by that. I've rarely gotten the response from a patient that says oh,

I'm scared you got that on there, will you wipe it off because you don't want to get into the technology and tell them it's not really on my iPad, I'm just remoting in, but I rarely get a negative response most of the time.

DR. WHITE: So, they trust us to be responsible with their information.

MS. GALLAGHER: I was going to say that every major survey that I've seen indicates that the trust relationship is still with the physician, provider, and, so, that, of course, is something that we need to honor, but, yes, they do generally have trust that if that technology is implemented that the provider is doing it in a way that it's secure.

DR. WHITE: Okay, so, also thinking about the different people that we serve, good question: How can mobile health benefit underserved populations, especially patients with chronic conditions and adherence issues, patients who don't have coverage? We all take care of these folks, we all know that they maybe don't have access, they may not even have access

to information in the way that folks normally do, but they may have their cellphone that they get texts on. That's a link for them. Have you all seen in your experiences ways to connect with populations that we haven't been able to connect with before or ways that we can serve them better?

DR. HEILMAN: Oh, I do think absolutely, that mobile technology will help especially in things like home monitoring. We have high-risk maternal patients that we're trying to monitor from large distances and if we can just monitor fetal heart tones and things like that to know things are going well, that's a benefit.

Chronic CHF patients who are going home, just being able to record their weights on a daily basis to see what's going on, we have a grant submitted to kind of kind of help monitor that and get that infrastructure set in place. Monitoring COPD patients or asthma children who are in certain areas that may not have rapid access to their physician monitoring peak flows. Those are some of the great things that I think are on pipeline coming our way that will be leveraged by using

mobile device technology that will help us to provide better care to those rural areas.

DR. WHITE: Okay.

DR. TASHJIAN: I can think of 100 different things we can do. We haven't done them because we haven't figured the security out yet, and, so, that's why I'm really delighted to be part of this because if we can figure the security out, and I think we can, I think the sky's the limit and communication is going to be the next major leap to providing better care.

DR. WHITE: Great. Wow, I like that.

So, I like this one. I like a lot of these. How do you keep track of who's accessing your records remotely and what if someone quits? Ooh, that's good because we have people leaving our organizations all the time, and especially if they've got their own device, yes, maybe you can change the password, but is there a way to make sure that that happens in a timely way? What are you all doing with that?

DR. DeLaROSA: For us, the security, it gives you this little icon that comes up and it says you're

about to access a record, are you sure you want to access this record? And then you're imprinted and then it says this will be marked that you have reviewed this exam.

DR. WHITE: Ah.

DR. DeLaROSA: And, so, now then there are two icons that go on at the beginning and at the end now that you have been there. Your name, your ID, et cetera, you're logged on, and I think we're cautioned and educated that if you leave a computer to logoff because somebody else could come on and can use it, et cetera. Those are the ways of the security that we have in regards of knowing if somebody's been on there or not on the record.

MS. SHAFFER: We also go ahead and take their name and password out of the VPN so that way they can't get through at all.

DR. HEILMAN: Our HR software, once someone's terminated in the HR software, that feeds into our EMR and everything else that has passwords and deletes those, and, so, they can't beep you in, they can't log

in, and then the mobile technology third party, we have on our devices that we've partnered with, we're able to actually wipe the devices if we want to.

MS. GALLAGHER: So, what Dr. DeLaRosa was talking about is the actual implementation of a security audit log where we can log every access to patient data, even if it's a read access, and health care is dealing with an upcoming regulatory requirement for an accounting of disclosures which would require us to be able to log, track, and report on not only the disclosures, but the accesses to the patient data. So, that's something that employees should be knowledgeable about and should be trained about because even if there isn't an immediate indicator, they should know that that data is being logged.

DR. WHITE: Okay, go to Chris.

DR. TASHJIAN: I was just going to say having the ASP model really helps that because we don't have to keep track of that, our vendor does, and, so, when it came to meaningful use and doing the security aspect, we had to do the security that happened on our campus, but

all of the technology security, all of the access issues were handled by the ASP environment. So, again, I can't recommend that more.

DR. WHITE: Okay, good deal.

A couple of you mentioned this in your initial comments, but we'll lead back to it. Can you speak to the security issues associated with using Wi-Fi to input confidential information into an online database? Some of you mentioned using, getting access to public Wi-Fi and stuff like that and it's become more noticeable in the past year or two, something like that. Experiences with that that you want to share?

MS. SHAFFER: Because most of our providers are out in the field, they want to be able to download their information so that everybody in the office can see who needs to see, but there's a challenge with that because you don't, you're a little uncomfortable with them going to the McDonald's or Starbuck's and logging on. There are policies we have about not allowing them to do that, but it's difficult to monitor that and regulate it. So, that's a huge challenge. We give out

Sprint cards, but sometimes that's not always very reliable either. Coverage, like I said, even in New York City, can sometimes be a challenge.

DR. WHITE: So, it seems like it's got to be at a software level, right? You got to assume that the pipe that you're working on is compromised, even if it's not, and that you got to be passing information back and forth that people can't really intercept and look at it. Fair? Okay. Good deal.

So, I'll ask you a big question. A lot of these are specific questions; this is a big question. Where do you see the challenges in the intersection of policy and technology in mobile health? Discuss.

(Laughter)

MS. GALLAGHER: Well, I think that what we're seeing is that with regard to mobile technology specifically, it's very often being deployed before there even is a policy. And that's not the case with EHR technology and other technologies, but with mobile technology, people use it in their everyday life, they want it now, and they get it. So, in a lot of cases,

we're actually going back and catching up on the policies and it's not just documenting what the policy is, but what it should be and at the state that we want to get to regardless of how we got where we are and the fact that we deployed these things before we were organizationally ready. So, I think that's a challenge, and, so, at HIMSS, we see folks coming to us for resources to help them do that.

DR. DeLaROSA: The challenge from the provider standpoint is when the technology is there, you hear about it from a friend, a colleague, from someplace else, you want that right away. It's just like the iPad. It comes out next week or something – today-- and people want it right away, but then the policies aren't there yet and then, all of a sudden, there's a disconnect between administration and the policymakers and the physicians that why don't we have it yet? We need it now. It should have started yesterday and it's going to take months to implement to make these policies. So, it is a challenge that we face that, as you know, as physicians, we want things now for our

patients.

DR. WHITE: Well, either you don't want it, it's like no, no, don't want it, don't want it.

DR. DeLaROSA: Don't want it.

DR. WHITE: And now it's like why don't I have it? Yes.

DR. DeLaROSA: Exactly. So, there is a problem. So, and we wish we had policies in place or there was a standardized place that had policies that you would be able to take from them and sort of like a whitepaper, and then pick what you wanted from it to make your policy.

DR. HEILMAN: I think we're faced with a little bit of a contradiction right now because we're trying to free up technology information and data as much as we can, join the Health Information Exchange, get this information out there, push it out to everybody's mobile device, but, at the same time, don't violate any HIPAA rules, don't do anything. So, I'm going to put policy and governance in that says make sure you're secure as you possibly can be, but at the

same time, I'm going to demand you free that data up and push it out as much as you can. So, that's where I think some of those crossroads are coming into.

DR. WHITE: A lot of folks have kind of argued for a new social compact and social understanding around that the context in which we handle information now is so much different. So, unfortunately, got to get people to think about that all the time.

So, let me go from one big question to another big question. We've been talking a lot about how we currently the devices and what we've seen in terms of value. One of the forward-thinking things that people were discussing are Accountable Care Organizations. So, for Accountable Care Organizations, do you think mobile health applications would help the communication and transition of care? And I know the answer is yes, but then could you say a little more about that?

DR. TASHJIAN: Well, I touched on it earlier, but let me just take an example of this. We're all now being looked at as how many heart failure patients get

readmitted within a month, within six months, whatnot. I think communication is going to be the big key that reduces those readmissions and reduces the morbidity.

And, again, somebody was talking about entering weights and transitioning back and forth, communicating those so we know when to reach out. I think mobile or otherwise, that technology is going to, by enhancing this communication, we're going to catch things before they get too far down the line. So, it just seems reasonable to me that it's going to decrease the cost of care and, in fact, we're counting on it because as an independent clinic, we've already signed some total cost of care contracts, we're using our patient-centered medical home, we're using our technology, and we're basically betting the bank that it's going to pay off and we think it will.

DR. HEILMAN: Yes, I attended a lecture at HIMSS this year actually that was given by the people at Kaiser, and they were just talking about how they were able to leverage e-visits essentially because it's basically a capitated model where opening up that line

of communication and not worrying about being reimbursed for the visit, if you take that out of the equation, patients can communicate with their physicians a lot more freely, back to capturing those illnesses early before they go too far or treating those simply cases quickly to avoid the office visit, to avoid the ER visit and avoid those additional costs. Huge win.

MS. SHAFFER: And especially, too, when you bring homecare into the mix, we have telemonitoring and we've caught many patients who have been in CHF and trying to get them standing orders to be treated for home, and we've kept them out of the hospital that way, which is definitely cost-effective.

DR. DeLaROSA: The challenge that I see is that it's difficult to educate administrators about this. It's interesting to get all this data, but you need to have somebody to interpret the data to feed it back and then they don't see the ROI in hiring another person who is not producing and I've heard it from several hospitals, the investment of putting the person in there to interpret this data, what's our ROI on this,

and there is significant, as we hear, but people from readmission, getting them back in the hospital, but that is the next step of how do you get administrators to understand that aspect of that, interpret the data?

DR. WHITE: And do you think we can do this without good mobile technology, without good communications that we're going to be able to coordinate care better? I know I'm asking a biased group. It's a small sample, sorry. But that's okay.

MS. SHAFFER: I don't think that's possible, no.

DR. TASHJIAN: And, again, it's another tool in our armamentaria. As physicians, and, unfortunately, I've been here long enough to see things come and they do help and we make these transitions, and I think this is just another one of those that's inevitable.

DR. WHITE: Okay. So, I'm going to ask you one that makes me a little nervous, but it's near and dear to my heart given what I do. Discuss the value of academic research in this field. (Laughter) I'll let you hang, it's good. (Laughter)

DR. TASHJIAN: I will just say that as a practicing physician, I don't do academic research in general, but anything you can give us to help us is greatly appreciated. (Laughter)

DR. HEILMAN: Well, back to Dr. DeLaRosa's comment, I think if we can get published articles on the ROI and the benefit to the patients and the benefit to the organizations that institute this sort of information from research, all for it.

DR. WHITE: Helps push you along.

DR. HEILMAN: Absolutely.

DR. WHITE: Published articles on the value or on the quality of care, that it makes it safer or that it makes it more effective also helpful?

DR. HEILMAN: Absolutely. As payments models are being shifted to being reimbursement for quality, if you're saying the only way you can really attain those goals is by leveraging this technology, why wouldn't you go for it?

DR. WHITE: Gotcha. Okay.

MS. SHAFFER: And there have been some

published studies on telehealth and re-hospitalizations. So, it's out there.

DR. WHITE: Okay. Basically, when it's there, it helps you make the case to the executive's leadership of your different organizations that I can move this forward or, in Chris' case, maybe it will actually help him think about oh, maybe I can deliver care this way or do this differently and it's going to make a difference in what I do. Okay. Good deal.

Get back to the mundane here for a little bit. What kind of technical assistance do you receive for your mobile device since there are always upgrades and new functions going on and, again, Steve started to touch on this. We don't do that, we don't do that, okay, we do that. So, I mean, Chris is probably his own IT Department, right?

DR. TASHJIAN: I was going to say we have Gordy.

DR. WHITE: Yes.

DR. TASHJIAN: Gordy is the IT Department. He handles all of the access to the Web, he handles the

mobile devices, he handles everything, and, again, it works for us because we use this ASP environment. So, we only need to manage what's onsite, what's in our hands. Everything else is managed by Cerner, our vendor, and that works very well for us.

DR. HEILMAN: We have a fairly significant helpdesk that gets lots of calls.

DR. WHITE: Yes.

MS. SHAFFER: We have a large IT arm in Montefiore, but we also have our own little IT force right in our homecare agency, so, we're very fortunate. So, they handle a lot of the technical aspects of the laptops.

DR. WHITE: Yes, okay.

DR. DeLaROSA: And we have, it's about 1 IT per 35 health care providers, and is that sufficient? I don't know and I don't know of any data to show that you need so many IT per provider. I don't know if there's any data out there on that or if there should be, but that's how it is and it's a constant push for, again, to get more IT, and, again, you get back to the issue of

what is the ROI of hiring another person who's not going to be bringing income and then it goes back to the change and what value is. Value is quality over costs.

DR. WHITE: There you go. All right, last question. What are the main barriers besides costs that hinder the spread of innovative health technologies? Pick one.

DR. DeLaROSA: I think one of those from a provider standpoint is that many people don't want to change. Change is hard and it's not just in senior physicians, but it can be in younger ones, but most younger ones, they're texting on their way to their interview. I mean, that's what they do, but for senior physicians, change is hard and they don't want to change. I've done this for 30 years this way and it works, why should I change now from writing on a note or a pad? Those are the issues I see as a challenge.

DR. HEILMAN: I agree. Again, culture is probably the first obstacle we face on most things, but then it's just prioritization. I mean, there are over 400 projects on the project list in our IT Department

and we're having to go through and say limited manpower. Not costs, but manpower, which ones are we going to go after first? And, obviously, every physician and every practice thinks his initiative is the most important, whether it's his registry, his database, his new way of documenting cardiology. All of those have high priorities, but you can only tackle on so much per time and you have to really prioritize which ones you're going to go after first.

DR. TASHJIAN: We're small enough that we can tackle the culture issue, but where we really struggle is this mushroom of opportunities that sits in front of us. How do we choose the right one? How do we choose the ones that are actually going to help us because we really can't afford to go down the wrong road, we need to pick the right ones and for the right reasons. So, I think that's our biggest concern.

MS. GALLAGHER: So, for the IT Department, I think the broader discipline here is the management of disruptive technology, so, things that aren't part of the workflow now that we want to integrate into the

workflow. And too often, the IT folks are focused on management of the network and micro level things, but that discipline so that they handle the next new technology or new opportunity in a repeatable manner, in a manner that they can understand and communicate to their executive management.

DR. WHITE: Excellent. All right. Well, clearly, you have health care providers out there that are ready, willing, and able and excited to take these technologies and use them to deliver great care and also equally clear to me, which I'm really grateful for, fully appreciative of the issues that go along with using these and the responsibilities that come. So, I hope you will join me in thanking our panelists.

(Applause)

So, we're going to have a break and we're going to get together in 10 minutes. Okay, 10, 15 minutes. Thank you very much.

(Recess)

MS. MARCHESINI: If I could have everyone in the room to find your ways to your seats, please.

(Pause)

MS. MARCHESINI: We're about to start the third panel focusing on Real World Mobile Device Privacy and Security Practices, Strategies, and Technologies. The moderator for this panel is Mr. David Holtzman with the U.S. Department of Health and Human Services Office for Civil Rights. He joined the Health Information Privacy Team at OCR in December 2005. He is currently working on the development and enforcement of the HIPAA Security Rule. ONC is also working in collaboration with OCR for a larger privacy and security mobile devices and to help put on today's event.

Prior to joining HHS, Mr. Holtzman was the privacy and security officer for Kaiser Permanente's Mid-Atlantic Region, where he was responsible for implementing and directing the continuing compliance with the HIPAA Security and Privacy Rules. Ladies and gentlemen, please welcome Mr. David Holtzman.

(Applause)

MR. HOLTZMAN: Thank you, Kathryn, and I'm

very glad to be here and thank the ONC for inviting us to participate and partner in this important discussion, and at this time, I'd like to invite our panelists to come up onto the stage. Sharon Finney, who is the data security officer for Adventist Health System in Orlando, Florida. Dr. James French, who is a hospitalist and health informaticist with Triad Hospital. Terrell Herzig, who's with the University of Alabama Health System and serves as their chief information security officer. Adam Kehler with Quality Insights of Pennsylvania, where he is the well, informatics jack of all trades. And Micky Tripathi of the Massachusetts Electronic Health Collaborative, where he is the CEO, and Micky can better describe all the wonderful activities that his organization leads and makes change in.

So, at this time, I'd like to turn to our panel and give them a few minutes to introduce themselves and describe, give us more information about their organizations.

Sharon?

MS. FINNEY: Thank you, David.

As David said, my name is Sharon Finney. I'm the corporate head of security officer for Adventist Health Systems. We are one of the largest health systems in the United States. We cover 10 states, 44 hospital facilities, approximately 300 physician practices, urgent care centers, home health, DME, and a long-term acute care. We have about 65,000 employees in our environment in support operations for over 12,000 physicians and their office staff, as well as a contingent of other third-party users in our environment. The environment that we've worked in for the last -- at least at the time that I've been at Adventist, which has been the last four years, is it's amazing to me that we've been utilizing mobile devices in health care for a long time. They're all over our hospitals and our clinical care units today, but there are devices that the organization has held and owned and bought and purchased and secured.

As we've moved forward to look at how we integrate these mobile devices into our environment, we

are really taking the same approach that we've taken to every other technology that we look at in our environment today. So, as we looked that down, we looked at them from a risk-based perspective and said how are people going to use them? Who's going to use them? What data are they going to access? Will it reside on the device? How mobile will it be? Where will it go? How can it be transported from that device to other devices? So, we've applied the same risk assessment methodologies to these devices that we have to any technology that we've implemented. And as a result of that, we've kind of separated this into several categories.

The first is that we've defined our user population that wants to use these devices into two basic categories: there's a category of users that wants to use it in the clinical care continuum and to treat patients and bring their own devices in and then we have more of a business user that wants to use it. So, our executives want to bring it in and they want to use it like their laptop. So, those are two very

distinct different use cases in the environment and two very distinctly different sets of data that those users would access. Your executive users have a tendency to lean more towards your unstructured data in the environment and your clinicians generally will lean more towards your structured data in your electronic health records and other systems that are used to treat the patient.

As we looked at that, we also categorized the devices into personally-owned devices versus devices that we will purchase and buy and own ourselves and we've taken basically two independent strategies with that is that for the devices that we will own, we will control them the same way we have any other mobile device or any other device that we implement in our environment. For those devices that are personally owned, we are taking right now more of a container-based approach to how we deliver to the mobile device. So, we look at it as being able to deliver a set of services to an individual that has a device and we don't really want to care what the device is. We want to secure the data

and deliver it to the device when the user needs it, and I think those are kind of the important things and strategies around what we've initially done in our adoption of sort of mobile technologies at a high level.

MR. HOLTZMAN: Thank you, Sharon.

Dr. French?

DR. FRENCH: Hi, I'm James French. I'm a hospitalist. I'm working at Mercy Medical Center. I used to work for Moses Cone Health in Greensborough, North Carolina. We had a problem with our health care system. We had 800 to 1,000 med staff, our hospitalist program had 45 physicians, we would be doing anywhere from 50 to 100 admissions a day, and we had to deal with subspecialists under the constraints of length of stay and cost per case. We needed to improve communication. The med staff had everything from devices that were purchased by the hospital to devices that were personal. The med staff, some of them would be on the e-mail system, some of them wouldn't be. Some of them said I use a rotary phone, that's what I use; some of them had the latest and greatest smartphone. It was a nightmare.

We had to convey admissions, discharges, deaths, queries every day to the primary care doctors, we had to track down all the subspecialists to find out things about our patients so we can get them through the hospital efficiently, and at the end of the day, we developed a secure, encrypted, private texting network among our providers, as we think has really helped, and tied that into an online scheduling program that we've had a lot of success with, but this is the kind of health care communication needs that as a physician, this is what I see. We've been using pagers since 1970, and pagers are just not working anymore. But now we have the ability with the new smartphones to go into a whole new world of physician communication, and I'm just excited to be a part of that.

MR. HOLTZMAN: Thank you, Dr. French.

Terrell?

MR. HERZIG: Thank you. I'm Terrell Herzig, information security officer for the University of Alabama at Birmingham Health System.

To kind of give you an idea about what UAB

specializes in, we're an academic medical center, and I'm not sure if many of you have really come to understand how we have a lot of things going on here. But, basically, we have a couple of hospitals that we annually admit more than 42,000 individuals, and last year, throughout the health system, we saw more than 1.1 million patients. So, in addition to seeing patients and offering the best in care, we also have the mission of training new physicians and clinical staff. In addition to that, we also are very active in research, and by that, I mean we're one of the top NIH-sponsored research-sponsored hospitals. So, we have a lot of different missions in which certainly the interest in mobile devices are being greatly expressed each and every day.

Our facility does have programs where we equip devices and provide them to our faculty, but we also now are seeing not only the need for devices such as tablets and pad devices be used in patient care, but we also have an expressed interest by our research community to be able to use these devices on the

frontlines to be able to collect important research data. Couple that with the fact that a lot of our physicians are also some of those exact same academic researchers and they have facilities both in the hospital and then on the higher academic campus, and as a result, they have a need to access information from a host of different locations. Combine all of that with today's health care expansion and the fact that we're moving away from physical containers like hospitals and things like that and going mobile with our patient care, and as a result of that, we need to be mobile with our information.

Like what Sharon was talking about earlier, our strategies have focused on managing the data, kind of being device-agnostic because there's always going to be a new device come down the road, and, as a result, we need to be able to look at how that information is going to be used, what the need to gain access to that information is going to entail, and then we build use cases around that, and, as a result, if we can keep the data in the data center, but provide the same access

back to the clinician or physician, then we put our organization at a lot less risk.

Now, we started with mobile device technology and looking at different ways to protect it way back in 2005, when we started doing those risk assessments that everyone out there should be doing, and as a result of that, we identified mobile devices as one of our top 10 concerns and we've been working on it ever since. So, what we want to do is we want to adopt these devices; we want to make sure that they can be of use to our community, but, at the same time, protect that patient information and make sure that we do not result in a loss of data.

MR. HOLTZMAN: Thank you, Terrell.

Adam, you bring a different perspective from your vantage point. Can you tell us a little bit about that?

MR. KEHLER: Yes, I work for Quality Insights of Pennsylvania, which is part of West Virginia Medical Institute. We also are the Regional Extension Center for Pennsylvania, as well as Delaware, and we're also

subcontracted in West Virginia, for meaningful use to participate as the REC to help physicians as they transition to electronic medical records.

My role in particular, I focus strictly on privacy and security, so, helping practices meet that privacy and security requirement for meaningful use, which is conducting the security risk assessment and implementing updates to address those risks. So, I'm out there pretty much every day visiting with practices throughout Pennsylvania, both in rural, urban settings, mostly small- to medium-sized practices, everything from a one-physician office up to maybe a 15- or 16-physician practice. And, so, I kind of see the whole gamut of adoption of this technology.

There is definitely a lot of adoption of mobile technology both by small providers and larger providers. Generally, I mean, it's along the same thing that people talked about already. There's a lot of adoption of technology, and, often, it's the doctor gets a smartphone or an iPad and wants to try it out and start using it, and it's kind of I'll say a free for all

at that point, and actually looking at the security risks has not even actually occurred to many physicians and practices.

So, when I show up to do a security risk assessment, many of these practices have never performed a security risk assessment before, and, often, there's a bit of a hurdle to get past simply the complacency, the idea that well, there's no patient information on my device, on my smartphone or on my laptop or tablet, and, so, I don't have to worry about the security.

So, I would say one of the greatest challenges that I've seen with small providers is simply education and awareness, helping them understand that the different use cases for where protected health information may end up on your device. This could include information outside the electronic medical record system, including text messages. Many answering services send text messages to physicians to notify them. This will include patient name, phone number, some symptom information. Other documents that may be stored on laptops or tablets, e-mails, sending and

receiving e-mail, and those are downloaded to your device. So, with the risk assessment, we really need to go outside the electronic medical record system and look at all those use cases.

So, what I'll do with them is we'll talk about those use cases; we'll look at what controls are currently in place. Often, they have a passcode on their smartphone or a password on their laptop and they'll have anti-virus in place and they may delete the text messages when they're done with them.

As far as recommending additional controls, I found a lot of great value out of the NIST documents, Special Publication 800-53, including things like light listing software so you know what software is on that device and you've done your due diligence, and, obviously, encryption, VPNs, authentication, and things like that.

So, as I mentioned, with my security risk assessment, I would say about half of it is education; the other half is actually documenting security risks, and, so, that's one of the great challenges that small

providers face. It's just understanding what are reasonable and appropriate security controls.

AR. HOLTZMAN: Thank you very much, Adam.

And, Micky, you bring a slightly different perspective in your practice.

DR. TRIPATHI: Sure. So, good afternoon. I'm Micky Tripathi with the Massachusetts eHealth Collaborative. We are a non-profit organization that focuses on implementation services related to health information technology, both EHRs and HIE, to improve community health, which is our non-profit mission.

We work with a large number of physicians. We are the Regional Extension Center of New Hampshire, confusingly enough since we're the Massachusetts eHealth Collaborative. But we are also working as a contractor, just like Adam's organization is and other states, so, we're in New York, Massachusetts, our home state, and Rhode Island, and we have our headquarters in Waltham, Massachusetts, in the Massachusetts Medical Society Building, with whom we have a very strong affiliation. We also have an office in Concord, New Hampshire, and in

Providence, Rhode Island.

So, we're working with roughly 1,700 to 1,800 physicians actively right now on meaningful use optimization both as an REC, as formally as part of the REC Program, as well as through private engagements, although the work is largely the same. I would echo almost everything that Adam said in terms of what we experience. We're working also down at the very bottom of the food chain in terms of very small practices. We don't work with that many practices who are over four or five clinicians in the practice.

I think one slight difference between Adam and I, we were comparing notes before, is that at least with the practices we're working with in New England, amazingly enough, smartphone penetration isn't that high yet among the small practices. So, when we think of mobile devices, for the most part, it's about laptops. So, I'll turn to Adam to talk more about the experience with smartphones and the things that he's doing there, but I would almost echo almost everything he said in terms of what we're encountering on the ground with

respect to laptops and small devices.

MR. HOLTZMAN: Thank you very much, Micky.

So, the object of this panel for the next hour, hour and 15 minutes is we're going to engage in a conversation in how to discuss the use and protection of mobile devices in health care and specifically in actual medical practices. I'd like to invite those of you who are attending in-person as well as those of you who are watching this through a webcast, please submit questions to us. The panel is very interested in hearing from you and answering your questions and bringing issues that, so far, haven't been explored. Just a note, the discussions, the practices, and recommendations that some of -- I've already been handed a stack of questions. (Laughter)

The discussion of practices and the activities that the experts here are going to describe, they have not been evaluated by the Office for Civil Rights and they don't necessarily represent compliance with the HIPAA Privacy or Security Rules or represent guidance by the Department of Health and Human Services. So, I've

done my little disclaimer. (Laughter)

So, Sharon, how does your organization integrate different mobile devices into your organizational enterprise setting?

MS. FINNEY: Well, David, I think probably like most hospital systems today, whether they're probably small or large, most hospitals today provide some public Internet access in their lobbies and for their patient areas so their patients can bring their own devices in. And when these devices emerge, that's exactly what happened, they brought them in and put them on the public network, but what we started to see was we started to see more and more physicians coming in with these devices and then we started seeing some employees coming in with these devices and with the smartphones and the iPads and the Droids that are out there today, and as we saw this sort of evolving in our public network space that we provide in our facilities, we started looking at what they're actually doing using these devices. I mean, are they just using them for fun, are they doing Facebook and those kinds of things

or are they actually using them to work out of our environment and do productive things on them or just for sort of recreational use? And what we saw was that the user population was continuing to evolve into using these devices for more of that blended culture that we have today, which is where you move sort of seamlessly between your work and your personal life and you do it via this device that's in your hand.

So, as we looked at that, we started interviewing a lot of our clinicians and physicians and talking to them about how they were using these devices, and as our vendors that supply our electronic health record systems and our clinical systems also are evolving at this time and developing applications and mechanisms to be able to deliver their applications to these particular form factors, and, so, we kind of marched with that evolution and when our vendors came together and were able to provide us the mechanisms to allow that connectivity, we created in our environment a separate network, a segmented network for our physicians. So, that's a quality of service network

that when our physicians come into our facilities, they can connect their personal devices to that network. It's not the public network, they do have to register the device with us so we know who they are, and then at that point, we deliver to them sort of a higher level of service on that network than you would get in just our public area. And we're also able to drive to them sort of the same user experience that they have when they're remote, when they're out of the office so it feels just like they're sort of connecting to the Internet and coming into and accessing the clinical applications that they have available to them already from their home computer or other remote devices that they may have.

So, that's kind of where we started and then we progressed to also start to look at well, what about all these employees that are carrying around these Blackberrys and other devices that we corporately owned and given to them and what we found when we polled those users was that they really didn't want to carry two devices anymore. They didn't want their work Blackberry and their smartphone or whatever they purchased. For

the majority of the people, they wanted to use their own device, and, so, then we began to look at okay, so, now how do we deliver the services that those users need and deliver them securely to those devices and we chose a technology that would allow us to do that, and, as a result, we've migrated probably about 70 to 80 percent of all our corporately-owned Blackberrys and other devices to personally-owned and delivered services to those and allow them to use them in our network environment. They can connect to our public wireless or use their 3G, 4G service. We provide repeaters in our facilities for them to be able to use that.

And then so now what we're looking at is how do we increase those services to those devices because you give them a little bit and then they're going to figure out a new way to use it or something they can do better and stronger and faster with it, and, so, we've created some taskforces and things inside of our environment that allow us to collect a lot of that feedback from critical user groups that are using these devices and use that to also kind of fuel how we build

continuing relationships with our vendors and these device manufacturers so that we start to bridge that gap and progress down the path of being able to deliver what they need to do their work.

DR. HOLTZMAN: Thank you, Sharon.

Terrell, in your setting, another large setting, but with unique challenges, can you share with us how your organization integrates different mobile choices --

MR. HERZIG: Sure, absolutely. As I had alluded to earlier, we've got everything from medical students coming in with just about every device imaginable. If it's out there, we usually see it presented to us with the request to hook it up to our network.

Our approach has been to develop, of course, use cases to see exactly what these devices will need to interface with, what kind of data they need, and it runs the gamut, anything from simple phones to be used just for keeping up with other individuals, with communicating with other physicians, to I need access to

some resource out on a network device. So, what we did is we've put together a group of physicians, not unlike Sharon's practice, to actually identify these different cases, document them, and then that actually gave us a set of baseline controls that we need to implement, depending on what the use of the device is.

I think one of the things that's critical to note is that these devices are consumer devices that don't necessarily have a lot of security built in them when a user presents them. We have an obligation on the part of our organization to protect that health information, but there's a fine line there, too, not only from the risk perspective, but if you can take a device and you're converting it into a complete enterprise device, then what's the point in supporting these types of devices in your environment? So, what we've tried to do is evaluate, of course, how those devices will be used and put controls in place.

As a result of that, we've done a lot of things like what Sharon's group has actively done. You can't directly connect to our network unless, of course,

you bring the device in and we can make sure that the controls fit for whatever the different types of use cases are. We have a stratified wireless environment, just like Sharon's environment, we have a public Wi-Fi that's generally open to individuals for their general use, as well as our patients. We don't allow, of course, access directly back into our clinical environment from that particular segment, but we do then have different internal wireless networks that will allow you to interface and allow our clinicians to come in to our medical care systems with wireless devices that we have worked with them to put in place.

So, in light of that, too, some of the things that we're looking at now, we have questions, of course, about texting, everybody's interested in texting today. We have a communications system for paging and things like that. We have a very active interest in physician communications and the ability to kind of move away from pagers and more toward these smart devices. So, of course, the security controls we have in place help that quite a bit.

Our primary means of access into our system is we, too, want to keep the data in the data center. We really don't want data moving directly to the device. We feel like if we can keep the data off the device and into the data center, then if it's lost, it's much, of course, less risk to the organization, but also then it just makes everything a little bit more efficient to re-provision a new device and get it back in the hands of the physician or the staff member.

So, we have two key ways in which we bring people in. If they're outside our network, it's through VPN or Citrix. We require two factor authentication and I'd like to point out one our good wins here lately from a security perspective is that traditionally, everybody kind of hated the little dongles for two-factor authentication because it was something else you had to carry. Well, guess what? With the mobile devices, we can actually push that control out on the mobile device and make it part of that two-factor authentication. We actually when that went live at UAB, we offered about a week to do a swap out with our clinical staff to bring

in your old hardware tokens, we'd swap them out for software versions that run on mobile devices. We haven't stopped converting yet. We only advertised it once and we continuously have a whole flood of walk-ins every day and I'm proud of that because it actually increases security, but it has also increased the use and the ability of people to dual purpose these devices.

MR. HOLTZMAN: Thank you, Terrell, for that comprehensive answer.

Micky, your perspective is completely different. You don't serve as just one organization, you serve as hundreds. Can you tell us how you help these smaller practices and clinics integrate the mobile devices into their environment?

DR. TRIPATHI: Sure. So, we've always encouraged mobile devices in practices. From the very beginning, even though these are small practices, our recommendation was always that they used tablets. I won't name any brands, but your favorite laptop tablet, and we were always encouraging putting these into the hands of clinicians and we still think that that's the

right strategy because they do then use it and it's a great form of adoption for them to be able to use it offsite and going to the hospital, as Sharon was describing, and be able to sort of have as much of that seamless experience as possible so that they're really using the full benefit of the technology.

That said, we've become more acutely aware and highly sensitive to the security risks that are brought forth by that, not by any experience that any one of our practices had, but by an experience that we ourselves had.

So, about a year ago, we had a breach ourselves. Now, we're consultants and we perform implementation services for practices. One of our practice consultants had a laptop stolen from their car when the car was parked in the city and that laptop was not encrypted at the time. We were, ironically enough, in the process of evaluating encryption solutions, but as luck would have it, the laptop was stolen before we had decided on a solution and had deployed it.

Our initial thought was that all we do, we

don’t normally have sort of a full medical record on our EHRs, I mean on our laptops as consultants, but one of the things we do is help practices with data migration from practice management systems. So, I’ll have an old practice management or billing system and we’ll help them with the data migration from that to the new EHR and there's almost typically almost always there are a certain amount of rejections in the automated process, and, so, what we would do is help the practice remediate those rejections and then delete the information, try to do that as much as possible in the office and then to the extent that there's stuff that we can't accomplish in the office, put it on the device, take care of it offsite, and then delete all the files.

So, our initial expectation was, well, there couldn’t be that many records on there and it’s only demographic information, so, it shouldn't be a big deal. We, fortunately, had a very fresh backup of it and, lo and behold, we discover that there were a few patient records on there, mainly 14,475 individual records. That shocked all of us.

So, lesson number one, there is more on your laptop that you realize, even when you're in the position of trying to teach others, which is the position that we were in. Now, it was not clinical information per se, but it was PHI, it was absolutely PHI. So, we went through a huge effort then to sort of go through then the forensic analysis, through a mediation process, and figure out what we had to do to respond and be in accordance with federal and state law, as well as then figuring out what the go forward path was with respect to our own administrative processes, our physical safeguards, our technical safeguards, and then use that as a lesson learned for the practices.

So, a couple of our lessons learned that we tried to now implicate in the practices are, A, don't for a minute think that there's no PHI on your mobile device. Don't for a minute think that that's the case because you've got all sorts of other stuff there. If you're doing any kind of scanning, document management kind of stuff, there's almost always going to be some kind of residual there, despite what the vendor may

claim. There are many cases that, unfortunately, we find that the clinicians want to save stuff locally because they want to work with it at home. So, in that case, they may know that they're not supposed to do it, but it happens anyway. In some other cases, it's on there, but they have no idea or that they either don't know what's wrong or they have no idea. They think it's secure and it's not. So, that was certainly our experience.

The other part of it was really related to do you really know who has access to your information and what they're doing with it, which in our case, those practices, unfortunately, were the victims of a consulting organization who came in and they didn't really have a full appreciation of what we were doing and certainly in the electronic world, so much of it happens sort of under the radar. Certainly, if we were going to walk out of the practice with 14,000 paper records, someone probably would have noticed that. (Laughter) But the fact that it was on our laptop and everybody was doing the right thing, but we had this

incident, it was certainly a lesson learned and one lesson that we always give to the practices is you need to do a complete assessment, which is like the security assessment, but more from a real business perspective and understand who's in your practice, what they're doing, and what are they taking away.

The last thing was that it has to be about more than just administrative safeguards. So, we now have full, needless to say, we have full encryption on all of our mobile devices and that's what we are telling the practices they really need to have, as well, is just full encryption, whole disc encryption because they can have every administrative safeguard in the world, but something is going to happen. Something is going to happen at some time, and in our case, if that laptop had been encrypted, we wouldn't be in the situation that we found ourselves in.

The best thing that we can do, it turns out, for practices and helping them sort of get the message is describe our experience. So, this was an experience that actually was I wrote a column for the HIStalk's

Blog that then appeared in the *New York Times*. So, it got a fair amount of circulation, and, so, we described the experience to the practice, but we also described how much it cost us. So, it ended up costing us $300,000 to do the full remediation of this incident with the 14,000 records, we ended up having to send out patient notifications, we ended up having to do a lot of legal work, a lot of forensic analysis. We're a small organization, $300,000, and that was -- we didn't get fined by OCR, by the state government, or anything, that was just our cost plus about 600 hours of our staff time to do the full remediation and figure it out. And if all of the other stuff doesn't get the practice's attention, that almost always gets the practice's attention. So, that's almost our best, sort of the best tool now to convince practices to think much more seriously about where they are.

MR. HOLTZMAN: Thank you very much.

Dr. French, does your organization provide your physicians and both the staff or hospitalist, physician, or the referring physicians with devices or

do you allow your physicians to bring their own devices onto your network?

DR. FRENCH: Well, we've tried it both ways. The problem with handheld devices is that initially, it was like driving a car that was designed specifically for a mechanic, not necessarily for a driver. So, I have three or four boxes at home full of handheld devices that were bought for me by the hospital that I never used ever, and what's really great about Sharon and Terrell and their remarks is that now, we're trying to adapt systems to real-life experiences of physicians and health care practitioners that are using these devices.

We provide a subsidy for the physicians; we do not purchase devices specifically for the physicians. This is much, much better than actually buying devices we found. We have to try to make this thing work and the physicians have to be motivated to use them, but physicians will do something if it meets one of three criteria: if it makes more money, it if saves time, or if it improves patient care. If it meets all three

criteria, physicians will do it spontaneously. They won't have to be prompted. If it meets zero criteria, they'll only do it unless you threaten to fire them. So, you've got to use a system that will adapt to whatever that they're carrying and the hospital-purchased device, we found, just didn't seem to work out.

MR. HOLTZMAN: Thank you.

Adam, your experience is probably a little bit different. How do you advise your clients on bringing in devices, whether they're provided by the organization or they're brought in as under a bring your own device policy?

MR. KEHLER: Yes, I definitely see both out there, and, as Dr. French mentioned, these devices do often meet those three criteria, and, so, you will see practitioners spontaneously bringing in the devices and adopting them because they do enhance their ability to take care of the patient.

What I do with them is I really just guide them through the thought process of doing the security

risk assessment, thinking about the different scenarios you're using your device for, how that ends up storing protected health information on your device or you're accessing protected health information and what are reasonable and appropriate security controls to help protect that information? By adopting these technologies, there will always be an additional risk. We can't remove the risk. What we can do is we can reduce it to an acceptable level.

So, I mean, some of the things that I often advise them with is to go through that process, do it in a very thought out manner, and start with policy. Don't jump to the technical solution to find what is appropriate use for these devices, whether it be laptops or smartphones or tablets. Are you permitted to take them offsite, and, if so, what additional protections are in place? Is personal use acceptable on them, and, if so, how are we safeguarding our health information? Is it permissible to install other pieces of software on the device?

And once you've developed the policies and ensure

you're enforcing the policies because I definitely see a lot of policies that are on paper that don't actually hold any water as far as governing behavior, once you've done that, then you can look at okay, what are the technical safeguards because, as Micky mentioned, you can have all the policies in the world, but someone is going to lose that laptop and there will be protected health information on it. You can almost guarantee it.

So, then you look at the next layer, which is the technical safeguards and the greatest one there, you've probably heard 100 times today, but encryption. If your devices are leaving the practice, it's -- to me – it's hard to understand why you wouldn't encrypt the device, and when I talk to office managers and physicians and things, often, they're not even familiar with something like full disc encryption. They're like oh, what is that? Like how does that work and then we get into a discussion about full disc encryption and the specifics of that.

You have to be a little bit careful with that. Not all encryption is equal. As many people may

know with I guess a certain popular tablet, there's built-in hardware encryption, but with older versions, there are ways to get around it. So, I mean, really how valuable is that encryption then, even if it is AES 256-bit encryption? So, we have to look at that and I think with the smartphones, the consumer products, we're starting to get there. I don't think they're there yet. There's a few that have always supported full disc encryption, but I think they're playing catch-up with that.

And if you're familiar with the NSA's Project Fishbowl, which many people heard about at the RSA conference recently, they were looking for a consumer device that natively supported all of their encryption and security requirements and ultimately, they couldn't find one. I believe they ended up selecting the Android, mostly due to the open architecture and they were able to complement that with their own in-house capabilities.

So, we're not there yet as far as encryption, but I think we're getting there.

MR. HOLTZMAN: Sharon, could you briefly describe the some of the technical or technology that might be available for mobile device management solutions?

MS. FINNEY: Well, now, David, I'm from the south, so, we don't "briefly" describe anything. (Laughter) But we have looked at multiple mobile device management strategies, and from placing an agent on the device to container-based or what we call sandboxed approaches, which is really more of what you see traditionally in this space. If you have an iPhone, you have multiple applications loaded on that iPhone. For the most part, those are little sandboxes. You can operate within that application whatever you do in there, and then when you close it, it's gone. Okay.

The issue around, I think, mobile devices is as what Terrell alluded to, was this concept of the device or the data staying in the data center versus leaving on the device. When does the device become dangerous to me or a security risk? It's only when it has the data on it. And, so, what we did was something

that we really actually started applying in our laptop world in-house in our facilities. We have thousands and thousands of laptops in our environment, some of them we put on carts, some of them we do these rough books or things, these ruggedized devices that are made for health care, and then standard laptops that most people carry around, and we started looking at encryption, like most people, around these laptop devices. And as we looked at the use case for these various devices that we had in our environment, we found that a lot of the clinical ones didn't really have clinical data on them. They were just being used as conduits to get to the application or access to the data so that they could use the application. They weren't creating or storing anything locally.

So, what we did was create a strategy that said you know what; we're locking those devices down. We don't allow anything to be stored on the local hard drive, we lock it down, it has no access to network shares, we don't put Microsoft Office products on it because we put readers on there so they could read

documents if they need to, but we said, you know what, that device is for that use case and that's the way we're going to secure it. Now for the ones that are highly mobile we know, like mine, I can store data locally, I have a lot of materials on it, I carry it with me, that's fully whole disc encrypted and has appropriate security controls on it. With these mobile devices, we kind of took the same approach and we said if it's a device that we're only going to deliver a service to or we're only going to place an application on it and once that application closes and nothing is stored locally, then we really didn't feel like that we had to take a lot of management control of that device. But if it's a device that we're going to allow to enter our network and we're going to place it in our environment, we're going to allow data to be stored locally on it, then at that point, we began looking at some of the available solutions out there to take full control of that device.

I still think there are some issues around if that's a personal device because, I mean, if someone

signs a form that says yes, I understand, I give you permission, lock the thing if it gets lost, but then when it actually comes time to do that, it can be a little bit of a different scenario. So, we've looked at software-based solutions, we've looked at what the vendors natively provide in the environments, and they do provide security controls that can be implemented for these tools or for the devices, but they're very device-specific. If you want to go to something that isn't device-specific and be able to control multiple types of devices in the environment, then you're going to have to look at a third-party software solution and there are multiple ones that are out there that you can review that are all quite good, have come a long way.

MR. HOLTZMAN: Thank you.

Dr. French, do you have an IT staff that is dedicated to assisting your organization and the physicians that you support? And, if so, how do you keep your IT staff up-to-date on the never-ending parade of mobile devices, like the ones in your closet?

(Laughter)

DR. FRENCH: Well, of course, we have an IT staff. Who else would we yell at? (Laughter) No, physicians are really dumb when it comes to IT in general, so, God, if we didn't have an IT staff, the whole thing would shut down in about a day.

As far as keeping everything updated, because of what we did, which is having people use their own smartphones predominately for communication, we've eliminated a lot of the we've got to update the software, got to buy new units, got to look at different vendors. We kind of took that out of the equation. The only thing that we update is our texting platform, which we've designed. We really played a hand in helping design for the health care for our environment. So, they have been helpful, IT has been very helpful in pointing out potential pitfalls and making sure that we're in compliance and making sure that we're secure, but the whole idea is to get away from anything that could cause a snag in the operation.

MR. HOLTZMAN: Thank you.

Micky, I know that your organization is

primarily IT professionals. How do you keep your workforce on the edge with the new devices?

DR. TRIPATHI: Yes, as it turns out, we're not mostly IT professionals.

MR. HOLTZMAN: Oh. Sorry.

DR. TRIPATHI: We certainly have IT professionals. So, even better, and, so, we do have IT professionals on our staff who keep up with the technology, but we also live within the larger domain. The Massachusetts Medical Society is a pretty complex organization itself. They own the *New England Journal of Medicine*, they have tens of thousands of members, so, we have the benefit of being able to leverage the knowledge and expertise that resides there. Otherwise, it would be much more difficult, I think, if we were just a small, non-profit consulting firm out there on our own trying to keep up with all of this and also be in the position of advising practices. I would feel much less comfortable, I think, if I were in that situation.

MR. HOLTZMAN: Thank you.

Adam, a viewer from the Web has asked: Earlier, you went into, you discussed NIST and authentication. Can you briefly go into more detail about what kind of authentication you use on mobile devices?

MR. KEHLER: Yes, I don't know that I can quote the NIST documents verbatim, and, so, I won't try to, but I can talk about general best practices as far as authentication. I think one thing that I see a lot is, again, some complacency around the idea that the password protects all. I see a lot of organizations that haven't honestly put a lot of thought into password policies, and, so, we'll get a lot of weak passwords, like 1234 or 1 or the word password, kind of all of that. Yes, raise your hand if I've named your password so far. (Laughter)

So, I mean, we definitely want to layer our approaches and not just rely on that password. I do really like the idea of two-factor authentication, especially for remote access, because when we're coming in off the Internet, that does expose us to additional

risk. So, some things like, I forget who it was , sorry it was Terrell, mentioned, an app for the second-factor authentication as opposed to the dongle. I know those are becoming a lot more popular, especially with Web-based applications.

I would also encourage vendors and people looking at solutions to look at certificate-based authentication. I think that's a very strong form of authentication. You can actually authenticate the device, as well as the person, and I think that really would help a lot, especially for Web-based applications.

MR. HOLTZMAN: Thank you very much.

We've gotten several questions regarding texting. So, I'm going to survey some folks, just kind of short answer. So, the questions are essentially do your facilities or organizations have policies regarding texting and the use of devices to transmit electronic health information via text? And what about policies of photographing with personal cellphones?

MS. FINNEY: I'll take this one first, is

that yes, we do have policies around the use of SMS text messaging for our employees, and our policy is that it is at this time not a secure method that is to be used to transmit confidential or patient-specific information. It is capable of being used to be a notification system or an alerting system to allow someone to call back and have discussion.

The Joint Commission recently came out with a statement that stated that texting of orders was not permitted, that there was no way, and they had two issues with it. The first is there was no way to verify that the person sending that order is the physicians actually holding that phone. There is no way that the receiving clinician can verify that. And then, secondly, there was no way to get that information into the medical record and because as an electronic piece of the order process, has to reside in the medical record. So, that was their two issues around sort of SMS text messaging. So, that's our policy regarding that.

And then the other piece of the question?

MR. HOLTZMAN: Use of the smartphone for --

MS. FINNEY: For photographs. We've actually had some incidents around this, and, so, it's we consider that, as we do the use of any device. I mean, they could easily do it with a camera. I mean, they could have a pocket camera just as well as they could have their iPhone or their cellphone with them, and there's no way that you can control that, there's no mechanism that you can put in place where I get an alert every time someone takes a picture. So, we educate our employees that taking photographs of patients or family members or in our facilities is not appropriate and not to be done. If we determine that an employee has violated that, then we have a sanction policy in place and we do sanction employees for violations of those types of things because I think really that becomes a point where there is sort of, that's an invasion of privacy of another person to do that, and, so, we take that very seriously.

MR. HOLTZMAN: Thank you.

Dr. French, I know that you come at this from a different direction. I mean, you were describing

earlier in our conversation how the use of the camera function is very important to your physicians.

DR. FRENCH: Yes, we do allow texting of protected patient information because our texting platform is secure and encrypted, which I think is a big deal. We do not allow people to text orders for the exact same reasons that Sharon brought up, but we'd take that one step further. We have work rules where you are mandated to text. When a patient comes into the hospital, you are mandated to text the primary care physician with the name, date of birth, and that they've been admitted and look in the EMR for the H and P. When they're discharged, same thing. If they die, same thing. If you have a question about the patient, text their primary care physician. So, we think that that's a really important piece to continue.

As far as photographs, absolutely. If the patient approves, it's a good way, because it's encrypted it's a good way to get that information out and not just photographs, and we can attach EKGs, we can attach films, or we'll soon be able to attach documents,

and I just see this as a big step forward to ultimately getting rid of the pager. So, yes, it is important in our practice.

MR. HOLTZMAN: Thank you very much.

MS. FINNEY: David, I have a follow-up to that, is that I wholeheartedly agree with Dr. French that text messaging is an integral part of the workflow in the clinical world today and I do believe that there are secure ways of being able to utilize that in a workflow and many more technologies are emerging around unified communications that are going to bring that even more tightly together. As we've tried to eliminate the number of devices that our physicians have on their back belt every morning when they get up, I don't know if you guys have seen a nurse lately on a floor walking around, but I feel like I need to put on a back brace on them and give them something to hold themselves up from all the devices they have strapped on them. And I think that's what unified communications and texting, I think, is just scratching the surface of that, is really going to give us in the clinical world and being able to

deliver that in a secure fashion, and it's something that we're investigating, as well, is how we continue to deliver that.

MR. HOLTZMAN: Thank you.

MR. HERZIG: David, if I can elaborate on that --

MR. HOLTZMAN: Oh, sure.

MR. HERZIG: Just a minute or two, the same kind of statement that Sharon and Dr. French are making is the fact that yes, for texting of orders and things like that, absolutely not. I think the directives are clear on that. However, I think organizations are going to increasingly want to use text. I know our research-based community wants to set up a rapport with today's modern users and will be able to use texting as a way of actually gathering some research data and things like that, and certainly in following up on patient care, there are some potentials there. Again, our organization is approaching it from a very careful process, we're looking at tools we can integrate into that unified communications process that are secure and

encrypted and can work with -- you don't have to put a lot of PHI in a text message to still have an effective text. So, again, we're looking at integrating secure products in with our existing unified communications product.

MR. HOLTZMAN: Adam?

MR. KEHLER: And there, if we can differentiate between SMS texting and just overall messaging because, Dr. French, correct me if I'm wrong, but the solution you've put in place is not necessarily SMS texting, it's a layer over that, it's a messaging platform, and I think that's a good point or good area to differentiate because there are certain risks with just straight SMS texting versus the encrypted solutions that we're discussing here.

MR. HOLTZMAN: Thank you, that's a very important distinction.

DR. TRIPATHI: David, I had just one other comment. I guess one of the things that concern me with just this topic is that one of the biggest enemies of security, I think is, and perhaps, the biggest enemy, is

convenience more than anything else. It's not that people are intentionally violating it because they want to violate it, it's because they're trying to do their jobs and they have a set of tools that make things incredibly convenient and that's becoming more and more the case with the different technologies in place, and, so, any time we try to have top-down policies that tell people you can't do the thing that's incredibly convenient, I just worry about what really happens on the ground.

And, so, at least our approach, and I know it's a very simplistic example, because we don't do the wide range of things that clinicians are doing in a complex hospital, but was to really rethink our strategy and to work it from the bottom up to ask the frontline people how do you do your day-to-day life and now how do I integrate a set of tools that are going to as much as possible keep your work as convenient as possible so you can get your job done?

And, I mean, I talked to a clinician yesterday who's an emergency department clinician, and

he takes hundreds of photos, hundreds of photos on his iPhone, and well, first off, he had a question I didn't have an answer to. Is a photo without any identifying information on it PHI? Joy Pritts says yes. (Laughter) Dr. French says no. This physician actually didn't know, and he said he wasn't sure how much he cared. He's an emergency room doc, he gets the patient's permission, he takes a picture of a rash, sends it to the dermatologist, gets an answer right back, and feels like I did the right thing. I did absolutely the right thing. So, how many other examples do we have of that kind of thing and how do you prevent it? I think there are some real challenges that are going to get to be a bigger and bigger challenge.

MS. FINNEY: And I'll respond to a couple of those comments, is I do think one key critical thing that you mentioned there was he got the patient's permission. And that is, I think, the key differentiating factor there. If the patient gives you permission to, the same way that he could have said I want to consult with this other physician, let me have

them come in and look at you. It's the same thing; you're just using a photo to do it. I think it's the ones that we're concerned about and the prohibiting factors of our policies is to ensure that our employees are aware that that can potentially be a violation of someone's privacy if you don't get their permission. And there is definitely a use for photographing of things in a clinical setting. Wound care is an excellent example, to measure how well a wound is healing over a period of time and we have cameras that we provide to some of our clinical staff. That's exactly what they do, that's then loaded into our medical record, and then it's deleted off the camera itself. So, I don't want to minimize the impact of being able to use photographic materials and devices in the clinical setting, but it's about using them properly and ensuring the patient is aware of exactly what is being done.

DR. TRIPATHI: So, that deals with the privacy, but not the security aspect of it. I think the other angle that makes it I think difficult in dealing

with small-practice physicians as they're trying to make this transition is they're coming from the fax world a lot of them, right, and with faxes, they don't meet any of the standards that we've talked about. So, the very reason you said you won't allow someone to text, is you could not apply that same logic to a fax, but people are faxing hundreds and thousands times a day in their practice. So, I think it's difficult for people to make the mind shift of saying wait a minute, I could do it in a fax, but you told me I can't use it on this mobile device. That's not going to work. I'll either go back to faxing, or, more likely, I'm just going to do it on the mobile device.

MR. HOLTZMAN: Well, this conversation certainly has shown us some areas where we need to have some further discussion about securing information not just in storage, but in transmission, and what the patient authorization covers and the extent to which we can protect the information and our responsibilities.

Terrell, as we integrate more mobile devices into our organizations and of all sizes and scope, there

a number of security provisions that must be considered. For example, there should be some type of, perhaps, access logging. Also, how do we prepare for contingencies like a catastrophic event or downtime of a cellular system or the EHR that it is accessing into?

MR. HERZIG: That's a good question because I can tell you from recent experience with some of the tornados and things like that, we went long periods of time in Alabama without some of our cellular infrastructure because it was damaged in that weather and stuff. So, I think as people depend more and more on these devices, the point is is that we have to plan for high availability in use of those systems.

Within our health care facility, we have long since been planning, and as we built our infrastructure, we built it in high availability format, and as along to those the ends, the devices that we use in medical care with patients and especially biomed devices, which I know we haven't talked much about this morning, we look for the technology that will allow us to use internal wireless infrastructures, as well as those cellular

infrastructures in order to deliver that high availability need.

MR. HOLTZMAN: Thank you, Terrell.

Adam, how do you help smaller practices and clinics evaluate the cost versus the risk in adapting mobile technologies?

MR. KEHLER: Well, I mean, the approach they take in the security risk assessment is I'm focusing a little more on helping them understand the risks that they have and what I'll do is I will suggest certain controls to put in place, but, ultimately, you kind of have to leave it up to them to determine what's reasonable and appropriate, what the cost benefit is.

I actually have started using Micky's experience in some of my risk assessments where I'll say, I'll just kind of let them know, you know what, if you have a large breach, here's what can happen, and it's not just OCR coming and finding you. It is notifying, for example, if you have a copy of 1,000 patients on your laptop, it is notifying 1,000 patients and trying to track them down, it's putting your name

out there in the media, it's legal costs for determining what your requirements are not just for HIPAA, but also at the state level. And, so, I try to help them understand that part of the cost benefit scenario and then once you talk about that, if you're looking at $100 to encrypt a laptop, that really puts that into perspective.

MR. HOLTZMAN: Thank you, Adam.

With the remaining few minutes that we have left, we have a couple of interesting questions from the Web. So, Sharon, briefly [LAUGHTER], how do you handle videos from patients to providers for diagnosis, medical advice? A use case would be people who are being transported to the emergency room and the emergency medical technicians use a video link to advise the physicians? And, also, another question: Do you somehow keep or store these videos?

MS. FINNEY: It really depends because we operate across 10 states. We also have to consider state law, as well as federal mandates from a privacy and security perspective and what we retain and don't

retain. If it is germane and important to the treatment of the patient, then we would retain it in our secure medical records system as a part of that. Generally, with most of our video feeds that we receive like that, those are generated by the EMS company. That's their video feed to us, so, they really are the ones storing it, not us. We're just a viewer or a participant of that. And that's really how we would handle it. If we provided our own video uplinks to our EMS, then I would think that, yes, we would probably store them period of time, but at some point, we would roll those off, depending what the retention requirements would be.

MR. HOLTZMAN: Thank you.

Does anybody else on the panel have anything to add to that? Are they involved in the use case, as well?

(No response)

MR. HOLTZMAN: Okay, thank you. And the last question, I'm going to use my speaker's prerogative, one of the challenges that we've been seeing at OCR is when an organization allows physicians and other health care

professionals who are referring physicians or not admitting practitioners in the practice to gain access to the system. How do you manage the physical and logical security of mobile devices from those who don't normally access your system?

MS. FINNEY: In our environment, David, we provide a level of access to a broad spectrum of users in our environment. When we provide access to any physician, whether referring or admitting, they have to go through a process to obtain that access. So, we do put them through sort of some type of a credentialing process to obtain those credentials. In that instance, we would not provide them a level of access that would allow them to store or retain any data on the device they were accessing it from; they would only have view access or some type of access into accessing information, and then nothing would remain on the device itself.

So, I really wouldn't worry about securing their device per se, and then in the event that we also have a process that we use in our environment that's

called a dormant account review where we go through and any account that hasn't been used in 120 days is disabled and then the physician would have to, if they didn't use their account in that time, they would have to contact us and have those credentials reset. So, we kind of go through a little reauthorization process. But as far as having to secure the actual device, that's something I want to try to stay away from with that user population.

MR. HOLTZMAN: Terrell, I see you chomping at the bit.

MR. HERZIG: No, actually, I was just going to kind of elaborate. Very similar concept to what Sharon was talking about except we have an ambassador portal that our referring physicians signup for. We have that signup process so we can, of course, give them access credentials. We do give them two-factor authentication to get in, their staff, as well, for when they need access to it. And then they identify, of course, patients that they want to follow and things like that, and they're signed-up, as well, and then when

they access the portal, of course, it's over secure links then. So, if their device can support access to that Web environment over the secure links, then, of course, their device would work as expected. But, other than that, if they're just in the facility with a device, it would be treated just like any other public device, no special access or anything, that it's all through that portal environment.

MR. HOLTZMAN: Adam or Micky, you're provisioning the providers that are trying to gain access to these systems. How do you assist your clients in these roaming networks of hospitals that they're trying to gain access to? Okay.

DR. TRIPATHI: So, well, at least the thought process I was going through was with the hospital, the hospital is going to deal with that, right? So, that's one particular use case, and then so, the hospitals deal with that. I get a little bit more sort of confused concern about the practice who wants to allow a referring physician in and what are the shortcuts that they may provide to allow that? And given that they

don’t live in an enterprise, typically, now that maybe that there are just some barriers that can never really allow that, allowing with GoToMyPC or any of these kinds of software systems. Sorry, I shouldn't have mentioned the brand. I don’t even think that’s the actual name. But they certainly, I think, are in an environment where they're going to try many, many, many solutions to try to figure out how to do that again because it’s convenient, not realizing that it’s probably not secure, and not that all of them will work because their vendor has probably put in some protections, but sometimes, stuff happens and stuff gets through, and, perhaps, it’s the environment isn't as secure as was thought, and, so, they're able to use things that aren't as secure as they need to be. So, I think at least that’s really the biggest concern overall is how they would get access to an enterprise-type approach to allow that access.

MR. KEHLER: Yes, and I’ll just build on that. One scenario I do see is especially as it gets into practices with a few more physicians is they’ll each kind of put in their own solution for getting

access to their computer, each physician will use a different remote desktop program and kind of do their own thing. So, one thing I always encourage them to do is look at that use case and come up with a solution and standardize it, and any time you're opening something up like that, you're opening up yourself to risk. So, look at also not just locking it down, but look at visibility. How do we review and monitor access to that system? Some of the Web-based, remote desktop systems will allow you to generate alerts so you get an e-mail every time someone logs in or you can at least review the logs and reports because on one side, we have our preventative controls, but we also want to have visibility and awareness.

MR. HOLTZMAN: Thank you very much. Well, this has been a great conversation, and I know our time has almost run, but we do want to squeeze in one more question that we received from a viewer.

Dr. French, earlier, you made reference to encrypting text messages. The viewer writes that they are looking for ways to do this. How is this

accomplished?

DR. FRENCH: Well, I can't speak to the actual encryption process. We bought an application that it comes encrypted. So, and as far as controlling access and controlling people outside the system that do get these messages, all of our messages self-delete. So, you set the time period and then it deletes on its own. But all I know for sure is that the encryption has passed our IT people, and I don't want to look like an idiot, but it's so many bit encryption, I don't remember, and it seems to pass muster.

MR. HOLTZMAN: Thank you very much.

Well, I'd like to thank all of our panelists today. They've done a wonderful job answering questions off the cuff and thank you for sharing your knowledge with us. Thanks to Sharon Finney, Dr. James French, Terrell Herzig, Adam Kehler, and Micky Tripathi. (Applause) Joy will come up and give a few closing remarks, and we thank you for your participation and attendance today.

MS. PRITTS: You're welcome to sit or why

don’t you just sit, then we’ll be done earlier that way.

Well, I’d like to thank not only this panel, but all of our panelists today. They have been very informative. As you know, this is just one of the first steps in this project that we’re undertaking with our partner, OCR, in identifying these important privacy and security issues and solutions for mobile devices.

If you haven't had the time yet, we’d also like to thank our audience, both those people who are here in-person and who participated on the Internet. We have had a number of forums where people have asked us for more participation. Oftentimes, when we have meetings, there's only a little piece of time, like 10 minutes at the end, where people can comment. So, we really took that under advice. I want you to know that the idea for having more participation during the day actually came from audiences like you. We listened and we implemented it, and I know from our perspective, it has worked incredibly well. We received very insightful comments and questions from the audience both here and on the Internet that have really helped inform this

discussion. But this isn't the end of it. If you haven't had the opportunity to submit comments or questions yet, there is an opportunity to do so on the Health IT website, which is posted here for everybody to see, and that comment period will remain open until March 30. And, so, keep your cards and letters coming in. We are looking forward to hearing more from you.

We'd like to use this opportunity to also, once again, thank our federal partners. We are the Office of the National Coordinator, and I want to ensure you that we actually do try to do this. So, our special thanks to AHRQ, FCC, FDA, FTC, and from ONC to OCR for being here with us today and showing you that your federal government is very involved in this area and has your back. I'd also like to give my personal thanks to Kathryn Marchesini of my office, as well as MAXIMUS who provided a lot of valuable support to her.

The way you can tell somebody is doing a really good job is when you're on the outside a little bit and you feel like it was seamless. So, from my perspective, this was a great, great conference because

I had almost nothing to do with it and it went really well. So, I really appreciate all of their effort, as well as that of other ONC staff.

We'd also like to let you know that we want to stay connected and to continue to collaborate with you and here are a number of different ways that you can communicate with ONC through Health IT Buzz.

Now, given the date and that it's St. Patrick's Day, I'd like to close with a little bit of a revised traditional Irish blessing for you all as you're getting ready to leave for the day. May the road rise up to meet you, may the wind always be at your back, may the sunshine warm upon your face, and the rain fall soft upon your fields, and may your health information always be private and secure. (Laughter) Thank you.

(Applause)

(Whereupon, at 12:11 p.m., the PROCEEDINGS were adjourned.)

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2012