

**HIT Policy Committee
Privacy & Security Tiger Team
Accounting for Disclosures Hearing
Transcript
September 30, 2013**

Attendance

Privacy and Security Tiger Team

The following members attended the meeting:

- Deven McGraw
- Paul Egerman
- Dixie Baker
- Judith Faulkner
- Leslie Francis
- Larry Garber
- Gayle Harrell
- John Houston
- David McCallie, Jr.
- We Rishel
- Micky Tripathi
- David Holtzman
- Kitt Winter

Privacy and Security Workgroup

The following members attended the meeting:

- Dixie Baker
- Walter Suarez
- Tony Dorsey
- Chad Hirsch
- Peter Kaufman
- David McCallie, Jr.
- John Moehrke

The following members were absent:

- John Blair
- Lisa Gallagher
- Leslie Kelly hall
- Ed Larsen
- Sharon Terry
- Avinash Shanbhag

Presentation

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Thank you. Good morning everyone, this is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of the Privacy & Security Tiger team; this is a virtual hearing on accounting of disclosures. This is a public call and there will be time for public comment at the end of the call. As a reminder, please state your name before speaking so that – because the meeting is being transcribed and recorded, we want to make sure that we get your name. Also, please make sure you mute your line if you are not speaking. I'll now take roll. Deven McGraw?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Here.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Paul Egerman?

Paul Egerman – Businessman/Software Entrepreneur

Here.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

David McCallie?

David McCallie, Jr., MD – Vice President, Medical Informatics – Cerner Corporation

Here.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Dixie Baker?

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates

I'm here.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Gayle Harrell?

Gayle Harrell, MA – Florida State Representative – Florida State Legislator

Here.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

John Houston? Judy Faulkner?

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation

Here.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Leslie Francis?

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Here.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Micky Tripathi? Wes Rishel?

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Here.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Larry Gar – hi Wes. Larry Garber? Kitt Winter?

Kitt Winter – eHealth Exchange Coordinating Committee Chair – Social Security Administration

Here.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

David Holtzman?

David Holtzman, JD, CIPP/G – Senior Health Information Technology & Privacy Policy Specialist – Office for Civil Rights

Staff for OCR, yes.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Thank you. The Health IT Privacy and Security Workgroup was also invited to join, so I will take roll for that group as well.

John Houston, JD – Vice President – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

This is John Houston; I don't think I was called.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Okay, thank you John. So Dixie Baker has already been called. Walter Suarez?

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

Yes, I'm here.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Chad Hirsch?

Chad Hirsch – Information Security Officer – Mayo Clinic

Here.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Ed Larsen? John Blair? John Moehrke?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

I am here.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Hi, John. Lisa Gallagher? Sharon Terry? Peter Kaufman?

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Here.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Tonya Dorsey?

Tonya Dorsey – Chief Implementation Architect – Blue Cross Blue Shield, South Carolina
Here.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator
Leslie Kelly Hall? Mike Davis?

Mike Davis – Veterans Health Administration
Here.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator
Avinash – sorry, we're not ready for that. And we've also invited members from NCVHS, do you want to just announce yourself if you are able to join today's call?

Jack Burke – National Committee on Vital and Health Statistics
Jack Burke.

Sallie Milam, JD – Chief Privacy Officer – West Virginia Health Care Authority
Sallie Milam.

John Travis, FHFMA, CPA – Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation
John Travis.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator
Oh hi, thank you, that's everyone, are there any ONC staff members on the line?

Kathryn Marchesini, JD – Policy Analyst – Office of the National Coordinator
Kathryn Marchesini.

Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator
Joy Pritts.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator
Thank you Joy. So I do want to make an announcement that we have exceeded the capacity on the web. We are working through some issues and hopefully we will be able to get more people in. For the moment, the materials are available on HealthIT.gov, which is our public website. All materials hopefully are up there at this point for you to look through, until we are able to fix our WebEx issues, or Adobe Connect issues I should say, so I apologize and please bear with us. I'll now turn it over to you Deven and Paul.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology
All right. Terrific, thank you very much, Michelle, very much appreciate it. We apologize for the web capacity issue; I know it's affecting members of the Tiger Team and probably also members of the Privacy and Security working group and NCVHS. So what that means is that for those of us who are moderating each of the panels, we're going to have to be mindful the queue for questions may include folks on the phone who are not actually able to use the raise hands function. So it will be incumbent upon us to make sure that we turn to the participants on the line to see if they have any questions. So, just to let you know, if you weren't able to login, we apologize for that but we will make sure that you have a chance to answer – to be able to ask questions. And again, the question period, when we're not in public comment, is limited to members of the Tiger Team, members of the Health IT Standards Committee Privacy and Security Workgroup and members of the NCVHS Privacy, Confidentiality and Security working group. We will have a public comment period, as we'll note, in the agenda.

So with that, we have some introductory issues to get through today and we very much appreciate the interest in the work we're doing. We're very eager to hear from both the people who are presenting today as well as members of the public. For those of you who have not noticed, the FACA Blog is another place where we are collecting comments from the public on this set of issues. So, all right, why are we doing this? What's the purpose of this hearing? We are really trying to explore realistic ways to provide patients with greater transparency about uses and disclosures of their digital identifiable health information. We think, or at least we hope, that such exploration should also help facilitate implementation of the HITECH requirement that a patient's right under the HIPAA Privacy Rule to an accounting of disclosures include disclosures for treatment, payment and operations when those disclosures are made through an electronic health record.

We've established five broad goals for our hearing today. We went to gain a greater understanding of what patients would like to know about uses and disclosures of their electronic protected health information. What are the capabilities of currently available, affordable technology that could be leveraged to provide patients with greater transparency? How are record access transparency technologies currently being deployed by healthcare providers, health plans and their business associates, for example HIEs? What are other issues that are raised – or what were other issues that were raised as part of the initial proposed rule to implement what was in HITECH regarding changes to the HIPAA accounting of disclosure requirements and exploring in more detail the difficulty in making the distinction between uses and disclosures.

Those are our goals and in fact the questions that we asked each of our presenters to try to address, and to – I just got knocked up a network – those questions that we asked them to address are tied to each of the goals. So we're not – and generally we also asked folks to address them as part of the FACA Blog and as part of the hearing. My apologies, I lost – I lost connectivity, I'll try to reconnect. But it's probably a good time that I lost connectivity because I'm handing the reins over to Linda Sanches from the Office for Civil Rights of HHS, who's going to take us through some of the regulatory backgrounds so that we all have a good grounding on both the HIPAA Privacy Rules historically as well as what was in HITECH and what was in the proposed rule. So Linda, are you ready?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office for Civil Rights

I am ready. Thank you, Deven. I just want to spend a little bit of time with the background. I unfortunately am getting a terrible echo, so I'm having trouble speaking while listening to myself with an echo. The Privacy Rule requires covered entities to make available, upon request, an accounting of disclosures of an individual's PHI. And the individual can request an accounting of all PHI disclosed up to six years prior to the request. The accounting and this is in the current Privacy Rule, would include the date the disclosure was made, who received it and a description of the PHI, as well as the purpose of the disclosure. The Privacy Rule accounting requirement applies to disclosures on both paper and electronic, and that's regardless of whether the information is in a designated record set. We note this because this is an issue in the NPRM that was put out later.

So just so people understand a designated record set refers to the records that are used by a covered entity to make decisions about the individual, which are medical records or billing records. But under the current rule –

Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator

Linda?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office for Civil Rights

– the accounting applies to any disclosures made in any records that are held by the covered entity. Next slide please.

Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator

Linda, you're very much echoing and it's very –

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office for Civil Rights

Now there are exceptions to this right and the largest and most important one is the right does not include disclosures to carry out treatment, payment or healthcare operations, so that's a very large group of disclosures that are not covered. There are some other important exclusions as well including those that the individual authorized to be made, those made by a covered entity to a researcher as part of a limited data set when there is a data use agreement and several others. Next slide please.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Linda, before you proceed, if you're on a headset, can please pick it up –

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office for Civil Rights

– required us to issue some new rule making to implement some new provisions, the HITECH Act included. There were two important issues here. The first was that the exception from the accounting of disclosures made – treatment or healthcare operations would no longer apply when those disclosures were made through an electronic health record. So individuals would have greatly – access to information about disclosures. The individual would have access to a record of those disclosures for a shorter time period, instead of six years as it was previously, it – and the – the HITECH Act provided two ways an individual could find information about disclosures made through a business associate. One would be the covered entity could directly provide the information to the individual or they could provide the individual with contact information for the business associates and then be able to contact the business associate directly. – also required adoption of standards that would allow for an accounting of disclosures in electronic health record technology. Next slide please.

So the Office of Civil Rights then issued a request for information about how one would implement these in covered entities environment. After reviewing that information, the Office did release a notice of proposed rulemaking in 2010 and it would have changed the original – well, what is currently in the rule and incorporates the HITECH Act provisions. I don't want to spend too much time on this because we ended up deciding to go back to the drawing board on these discussions. But I do want you to understand what was proposed. There would be two new rights, an accounting of disclosures and the new "access report." Next slide please.

So the accounting of disclosures would be disclosures made of an individual's protected health information, but it would be limited to the information that was disclosed from a designated record set. And it would be disclosures made in both paper and electronic form by covered entities and business associates. So you see there is a link here with the electronic health record that is a broader right. There is also in the NPRM, a list of disclosures that would need to be included including for public health, law enforcement, government programs providing public benefits, etcetera. And there were some proposed exclusions as well including in the case of abuse, neglect or domestic violence, for research when there's been an IRB waiver and for health oversight, etcetera, including information that meets the definition of patient safety work product. So as you see, there is a long list of exceptions, in addition to these – exceptions. Next slide please.

Now the access report was a new concept and that would include, if the individual requested it, anyone who accessed an individual's protected health information in an electronic designated record set. So not just the electronic health record, but all designated record sets in an electronic form. And access would both uses and disclosures. Note that this right does not extend to paper records. It would also require changes to covered entities notices of privacy practices to inform the individual of this new right. And again there would be a proposed exception for information that meets the definition of patient safety work product. Next slide please.

OCR chose not to address the accounting of disclosures issues in the Omnibus Rule that was issued in January this year. And we are very happy to have this opportunity of me appearing to provide a more updated understanding of what issues there might be in implementing the accounting of disclosures requirement, in the current environment. And I will turn it over now to Deven.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Okay. Thank you very much, Linda. I think the only other points to add on this slide in terms of background are with respect to certification of EHR technology. ONC has made accounting of disclosures an optional certification criteria for EHRs in the new 2014 edition that was also the case for the 2011 edition. And the intention is really to allow complete EHRs and module developers with flexibility to innovate in this area. So, one of the things that we might be exploring in terms of technical capability is this issue as well. So now we are to the point we've all been waiting for, which is the opportunity to hear from our testifiers. I'm not online, so I'm just going to have to say next slide to the folks from Altarum, or count on them to keep up with me.

What we should have is the agenda. We have four panels today. The first panel will be the panel on patient perspectives. Each panelist gets five minutes to present; it is not a lot of time. In fact, I can almost guarantee you it will probably feel ridiculously short when you're in the middle of your testimony. We unfortunately do not have the capacity to grant anybody any additional time for a presentation and we are actually going to give you a 30-second warning. You'll hear a rooster crowing in the background at about four minutes 30 seconds, which means you have half a minute to wrap up the point you're on. But we have a generous or we hope a generous question period for each panel that will allow you another opportunity to make a point that you were not able to make during the question period. But we are, unfortunately, going to have to be very strict and forgive us, but that makes it fair to the other presenters, too. We're going to have to be very strict with the five minutes.

We'll continue to – so, questioners, as I mentioned in the beginning, are limited to the members of the three working groups. If you are fortunate to be able to be online, the way that you do this is to use the raise hands function to put yourself in the queue and then the manager of the queue will call on you. Again, because there are a number of us who are not able to be online, each of the panel managers will take – will request questions on the telephone and we'll just do the best that we can to make sure folks have an opportunity to ask a question if they have one. We don't have unlimited question time, so obviously try to be judicious in your questions. If somebody else asks a question that you were going to ask and your question has essentially been answered, then we ask you allow other people an opportunity to ask questions as well. Do not put your phone on hold, because the chances are pretty good we will get to hold music and none of the rest of us will hear, so if you need – but please also keep your phone on mute, if you are not speaking.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

This is Peter Kaufman; I was able to get on the web now, so other people might try.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Okay, that's a good point. If you were not able to get on the web, you might give it another go. I will do so as well. The first panel is going to be moderated by Leslie Francis. The second panel is going to be moderated by Paul Egerman. I will moderate the third panel, assuming I'm able to get back online and then Dixie Baker will moderate the fourth. We'll have a period for – next slide please – we'll have a period for public comment at the end of the session. Public comments are limited to a couple of minutes per person. We will also be strict about the time limit here, keep in mind you have an opportunity to provide written public comment on the FACA Blog, and we're very interested in having folks weigh in on that. Paul Egerman, I'm going to turn to you to see if there is anything that you want to add before we allow Leslie to start the first panel.

Paul Egerman – Businessman/Software Entrepreneur

Thank you very much, Deven. I just want to thank everybody for their involvement. This is a very important topic and that's the reason why we are having a little bit of technical issues. We did not expect as many people to sign on as they did. But we are very pleased that there is interest, especially pleased any members of the public who are involved in the call, the public comment at the end is extremely important. So let's get started with Leslie.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Okay, this is Leslie Francis. Can everyone hear me?

Paul Tang, MD, MS – Vice President, Chief Innovation and Technology Officer – Palo Alto Medical Foundation

Yeah, one quickie. Deven, since – this is Paul Tang, sorry, I joined a few minutes later, but I can't get on the web either. To help us out, if it is posted, would you mind citing which file we should be looking at as the speakers talk?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

What do you mean by which file?

Paul Tang, MD, MS – Vice President, Chief Innovation and Technology Officer – Palo Alto Medical Foundation

If they're going to showing some PowerPoints on the screen, are we able to access it through the web?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

You should be there should be – there's a main deck of PowerPoint slides that includes any PowerPoints that anybody had submitted to us.

Paul Tang, MD, MS – Vice President, Chief Innovation and Technology Officer – Palo Alto Medical Foundation

Okay, got it. Got it, thank you.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Not everybody is submitting PowerPoints, because we did not require them.

Paul Tang, MD, MS – Vice President, Chief Innovation and Technology Officer – Palo Alto Medical Foundation

Got it. Okay. So this one listed, accounting of disclosure, virtual hearing PowerPoint?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Yes.

Paul Tang, MD, MS – Vice President, Chief Innovation and Technology Officer – Palo Alto Medical Foundation

Thank you.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

One more thing, too, if you're not the person that's speaking, if you could please mute your line.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Okay, so this is Leslie and it's time to get going. The first panel on patient perspectives has three speakers, Mark Richert, who is the Director of Public Policy at the American Federation for the Blind. Dr. Deborah Peel, who is the founder of Patient Privacy Rights and Michelle de Mooy, who is Senior Associate, National Priorities - Consumer Action. And without further ado, let's start with Mark.

Mark D. Richert, Esq. – Director, Public Policy – American Federation for the Blind

Great. Thank you, Leslie. Can you hear me all right; is this coming through good enough?

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Yup.

Mark D. Richert, Esq. – Director, Public Policy – American Federation for the Blind

Excellent. Well thank you so much for allowing us to present today. When Deven mention about hearing the rooster at 30 seconds, I almost wondered if I could ask for different farm animal, I'm not sure that – it would be nice if you could tailor the warnings to each of us. That having been said, I'm not sure which farm animal I would choose, so we'll stick with the rooster, I suppose. In any event, the first point I guess I want to make is this. It's been my privilege to work for various organizations in the field of blindness and vision impairment for almost 18 years now, and I'm pleased to represent today the American Foundation for the Blind. AFB is not a membership organization per se; we don't have consumer members per se of blind men and women. But we certainly since 1921, have been working hand in glove with consumers and professionals in the blindness, vision impairment world, on a host of issues ranging from civil rights, technology accessibility, healthcare accessibility for sure, special education and on and on. As you can probably guess, we have a far larger agenda than our human and financial resources might warrant, but we do our best.

I only bring that up to say that yours truly, who has been blind all his life, I think we take the perspective that hopefully is obvious, but I think sometimes needs to be said. Which is just like anybody else with or without disabilities, folks who are blind or visually impaired have the same interest in this topic, about the privacy of our information, making sure it's secure, being interested to find out who in the world is taking a look at it, as anyone else would be. What we don't have, like every other population I think, is ready access to the information that allows us to do all of that, to verify for ourselves about the security of the information, such as it is. Who has had access to it, indeed, we rarely have fairly robust access to the information that is intentionally made available to consumers. So being able to specifically go online or using a mobile gizmo or what have you, being able to make sure we can review, possibly add to or fill out forms. Whatever; the technical inaccessibility of that stuff means that folks who are blind or visually impaired who can't get access to the text or otherwise interact with the forms, it means that they're shutout of that process.

But in addition to that, what is an obvious problem but can be fixed by adherence to certain technical standards for the posting of materials or the development of websites or the development of databases, etcetera, those solutions do exist. There is obviously this whole other issue of being able to figure out who it is who's taking a look at your records. And indeed one area that is often overlooked is that we assume that when we're talking about consumers with a small "c," consumers of all this information, we're talking about patients only. When indeed more and more folks who are blind or visually impaired, indeed more folks with disabilities generally, are in the health care professions and themselves need access to this information.

So the punch line for me is that I hope as we talk about the various goals, which I think are right on the money for what you're trying to achieve. There is this layer that should be on top of all of it, which is not a thought we have at the end of the day or not a thought for a separate conversation. But it is a thought that needs to be part of everything that we do now which is, okay, if we're talking about the health records, if we're talking about the technologies, how do we make sure, how do we triple check that folks with disabilities, whether they are the patient or whether they are the healthcare professional involved, can make use of this information as fully and completely as possible and interact with whatever means that are put before him or her to make that happen.

So often, these topics of accessibility are left to, as I say, a separate discussion. It's sort of, okay, that's an accessibility questions, that's over there. If that happens, then essentially that's 90% of the battle lost. What we need to make sure happens is that throughout our discussions today, we're always suggesting, okay, let's not forget the disability side of this, which is to say, anything we do needs to involve a recognition of and a willingness to explore the implementation of the various technical standards that are in fact out there. Are they perfect? No. And unfortunately, yours truly is not a computer or electrical engineer, but especially a computer coder, so please don't ask me any questions about how to code things effectively to make it happen, but those solutions are out there, and certainly we can, if folks are more interested – holy mackerel, that's really quite something. I'm now deaf in my right ear, too. Can I speak for the deaf and blind community at this point?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Oh, I'm sorry. You have about 30 seconds.

Mark D. Richert, Esq. – Director, Public Policy – American Federation for the Blind

Well, on that happy note, I am going to wrap it up, but thank you so much and look forward to the Q&A.

John Houston, JD – Vice President – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

I think the rooster's dead now.

Mark D. Richert, Esq. – Director, Public Policy – American Federation for the Blind

I certainly – I would vote for that.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

I'll turn the volume down, I wasn't sure how loud it was, and apparently it's very loud. My apologies.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Okay, thank you very much, Mark. And now the next person who gets to kill the rooster is Dr. Deborah Peel.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Hi everybody. First of all, thank you so much for including us in this panel. Many of you know the history of the accounting of disclosures and our bipartisan coalition was really at the forefront of getting this particular consumer protection into HITECH. And I just want to second our support for all of the technology to make information available to everyone, including people that are disabled. So, up on the website, our testimony is there as PDF, at the bottom of the list of meeting resources, including an appendix that shows our previous two letters to the Office of Civil Rights about the accounting of disclosures. So we've been really involved with this whole process from the beginning.

The whole idea of the accounting of disclosures was patients should absolutely know what their information is and what it is being used for. So one of the first things we have to acknowledge is that an accounting of disclosures doesn't mean anything unless patients also have a copy of what was used or disclosed. So that's an important point. But really I want to make several other points. First of all, there are technologies today and processes that are already underway for meaningful use and for data security that accounting of disclosures could sort of be added to or piggybacked onto to make the cost less, to make this cheap, to make this easy and it's very important to automate accounting of disclosures upfront.

So right now there is a massive data asymmetry that's really causing the current failures of the Triple Aim because trust innovation are hampered. And so in my testimony, you'll see a data map and the data map some of you are familiar with, Latanya Sweeney and Harvard have been working with PPR, to try to begin to map out where the data is. So we don't know – the point is the data map shows dozens of entities that get copies of our health information and more, and aggregate it, and in the meantime patients can't get any data. So we believe that it's a patient's right to have digital access that should be real-time and online for accounting of disclosures. We think that any delays, if there are any, for digital access to all PHI really should be under the control of the patient's physician. Here we're talking about the concept of an HIE of one. Patients have really been locked out of benefiting from health technology because we still cannot get our data, even though that was a requirement when HIPAA was implemented in 2001. So the idea of HIE of one uses existing technologies. We need to automate blue button and use direct secure e-mail so patients can receive and send their own data.

Physicians should be able to communicate with us directly without hindrance or delay. And the point of using these existing initiatives, Blue Button Plus, the Direct secure e-mail project, we can essentially create through the accounting of disclosures, the ability for people to get both the accounting of disclosures and the data. And so, in our formal testimony, we lay out the steps. But basically we need to automate the process of creating and transmitting both accounting of disclosures and PHI so patients can have their data in real-time to take real actions. Why do we need and want the data? We need and want the data for our own health. We need to be able to have independent agents and advisors, independent decision-making tools. We need independence from the institutions and data holders that currently control our information. We need to have agents that represent us, not the interest of a corporation.

So the point of the data is so we cannot only check for breaches, inappropriate accesses and errors, but so that we can have the data and applications and services will be developed for us. We'll create a new market where technology innovators develop tools that actually serve us rather than data holders, large institutions and others that want our data. At the very least, patients should be first-class, first-class citizens in health technology and healthcare and the only way that we can be first-class citizens is if we have our data and have it in real-time. I'd just like to point out that –

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

That's probably a good – I think you're at your five minutes.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Okay, can I say one last thing?

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

One sentence.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Even before Blue Button, MD Anderson was giving patients complete access electronically to all of their information and it absolutely enhanced care.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Thanks very much, Dr. Peel. The next speaker is Michelle de Mooy. Michelle are you there? Is Michelle de Mooy on the line? It looks like she's not. Is there a way to get her from the phone?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Leslie, it's Deven. I can send her an e-mail, but in meantime, just for timing perspectives maybe we could move to the questions.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Yes. We're going to move to questions and answers and hoping – so I am looking for hands that get raised.

John Houston, JD – Vice President – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

I have my hand up. This is John Houston.

Leslie Francis, JD, PhD – University of Utah School of Medicine – National Committee on Vital and Health Statistics

Okay John, you're on.

John Houston, JD – Vice President – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Great, I'm going to ask a very incredibly practical question because working for large provider and accounting of disclosures is always something that's a huge challenge. I'm actually interested in understanding, when a request is made for an accounting of disclosures, really trying to understand what the patient is looking for. Because I think a lot of people think an accounting should have an enormous amount of detailed information and others, in fact in reality is, what my experience has shown is that when the patient asks for an accounting, they're typically looking for one or two pieces of information. They typically already understand that who the individual is their concerned about maybe accessing the record and they probably have a pretty good idea already, or they maybe want some additional information about what information has been accessed. So I'd be interested in your perspectives on what really needs to be in an accounting of disclosures. And what, practically speaking, what an accounting – if the patient provides to us some type of understanding of who they believe may have looked at their record, who they're concerned with, whether that also should be an alternative to this idea of giving them hundreds upon hundreds of individuals in an access log.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

This is Deborah. We have thought about this a great, great deal and one of things that absolutely has to be in the accounting of disclosures is a copy of what's been used and disclosed. That's what we need. Now not everyone is going to want that, but everyone has a right to that and people can select it. If the process of every time there is an audit log made, a copy of the record and the log is sent to a repository that the patient has, either their own computer, a separate storage facility kind of like.

Michelle de Mooy – Senior Associate, National Priorities – Consumer Action

Hi, this is Michelle I'm here.

Leslie Francis, JD, PhD – University of Utah School of Medicine – National Committee on Vital and Health Statistics

I was just going to let Deborah finish this answer, and then we've got Michelle.

Michelle de Mooy – Senior Associate, National Priorities – Consumer Action

Yeah, sorry. I called in on the public line, my mistake.

W

That's okay.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Deborah, would you like to finish this answer quickly and then we'll –

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Oh yeah, yeah. So the point is, the point is, patients need their own data for all kinds of uses and once we have it, tools will be developed to slice and dice it and help us get our own decision-making input and compare cost and quality, donate our data for research. We need – we're the ones that know how we want to use our data and have the rights to this data, have had it for a very long time. And so it should be everything. People can use what they want of it.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Okay. So now we're going to switch to Michelle de Mooy from the Consumer Action and you've got five minutes.

Michelle de Mooy – Senior Associate, National Priorities – Consumer Action

Okay. Good afternoon everybody, I apologize for that, I called in on the public line in accident. I just want to thank the HIT Policy Privacy & Security Tiger Team for inviting me to speak today. Consumer Action, just for a bit of background, is a 40-year-old national nonprofit. We're based in San Francisco but have offices in LA and DC and the DC office focuses on advocacy for underrepresented consumers. And my work focuses mainly on digital privacy. So, I want – my – just to kind of narrow it down, I really focused my testimony on the first question, but I'm happy to answer and address other questions if asked.

Many, many consumers are unaware of the incredibly vast ecosystem of corporate and government interest that are now directly involved with the access, use and receipt of PHI. This long trail of entities continues to grow exponentially and has the potential, we think, to undermine the rollout of an eHealthcare system. Transparency is, of course, the foundation of democracy and at the heart of any social – successful social system. In our experience the focus of worry for many consumers is centered on the misuse of their data, whether it's the embarrassing revelation of sensitive data, information that could compromise their safety or be used to discriminate against them, which has happened, of course. Erroneous information in their records and the difficulty of accessing records to correct the information is almost I would say impossible at times, and the loss of data in electronic systems. Patients are also very concerned about medical identity theft, and rightly so, considering that over 2 million consumers were victims of it in 2010.

Hard to reach consumers, in particular populations that include the elderly and limited English speakers, face enormous disparities in the adoption and delivery of healthcare services for a lot of reasons. Chief among them though is an abiding mistrust in the accountability of government systems. When done in a way that is easy to use and understand, with full disclosure of names, dates, times and purposes, the ability to view entities that have used or accessed PHI becomes a very powerful tool for underrepresented consumers. Giving them not only a way to ensure that their patient privacy has been upheld but also a way to hold their healthcare and insurance providers accountable rather than what we view as relying on the fox to guard the henhouse. We think it's a check and balance that is long overdue.

In addition the healthcare billing system is notoriously flawed. At Consumer Action we hear frequently from consumers who are being hounded by debt collectors for erroneous medical bills. When they call their healthcare providers or insurance companies to get answers or find out why they're being charged for certain items or procedures, they're given very little recourse to dispute, aside from asking for an accounting of disclosures and being given that, but of course it's filled with unreadable numbers and codes. We think this is unacceptable and borders are predatory. Disclosure with specific names and purposes in real-time assure that the consumer has some leverage in determining what went wrong and whether or not the charges are justified. For many that we speak with and deal with, the healthcare system is a maze of confusing bureaucracy and we're not looking for disclosures that add to that. When they're in need of medical services, it's all too common for providers, be it doctors or insurance claims adjustors, to fail to give consumers critical information about this type of thing, including things like conditions, treatments and the cost of all of these things.

For example, consumers are frequently unaware of the economic rationale for medical treatment and how different information flows between different offices and including government entities, which are sharing more and more information about consumers and this information, is now being used to determine things like Social Security benefits or security clearances. We also think importantly that HIE access points should be included in disclosures in order to provide a true map of where the PHI is flowing. Giving consumers a way to view the internal workings of the healthcare system, if done in a way that is easy to understand, available in multiple languages, would ideally provide them with the same perspective as their providers and again, leveling a very uneven playing field right now.

We also just want to reiterate the point that a Harvard University study done last year found that increased transparency led to more patient engagement and involvement in their own care, kind of echoing what Dr. Peel said. In the same way, we think providing accounting of disclosures can give patients a way to engage more full in their care and their privacy. I didn't get the rooster; does that mean I should keep going?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

You were going to get the rooster in 12 seconds Michelle, so you have like 30 seconds left.

Michelle de Mooy – Senior Associate, National Priorities – Consumer Action

I guess I just want to make the point again that we think it's important that HIE access points are included and we think the only way to achieve true transparency and accountability is to include that, including the name and purpose, every time the medical history is accessed, used or disclosed by any person or entity. And again I bring up the HIE access points because they are now the moderate switching post for PHI records.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Okay, so we're back now to the question and answer. In the queue I currently have Paul Egerman, Wes Rishel, David McCallie – let's see – Peter Kaufman, Walter Suarez and Linda Kloss. So we'll start with Paul.

John Houston, JD – Vice President – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Hey Leslie, can we finish my question first?

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Yes. John Houston's question was what information do patients really want? So, I guess that's Dr. Peel and Michelle de Mooy, if you've got any further comments on that.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Yes, this is Deborah. I just want to reiterate, we want and we deserve everything and people will make different choices about which part they use, but in order for us to be able to use the parts that we want, we have to have all of it. And we've always had these rights in the paper systems.

John Houston, JD – Vice President – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

But the question is, is that from a practicality perspective though?

Deborah C. Peel, MD – Founder – Patient Privacy Rights

It's very practical if it's automated, every time an accounting of disclosures entry is made, a copy of the data that was accessed along with the log can be just automatically sent to a repository that the patient creates or to a patient's agent. And then we have it and we can look at it and use it as we wish. Or the data could stay there and we could pull it from time to time or periodically. So it could happen automatically every time data is used, or the audit logs and the information could be held at the facility and that patient could pull them whenever via Direct.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Michelle, do you have anything to add to that or – ?

Michelle de Mooy – Senior Associate, National Priorities – Consumer Action

No, I think she put it well.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Or Mark?

Mark D. Richert, Esq. – Director, Public Policy – American Federation for the Blind

This is Mark. The only thing I would say is obviously we want to – obviously we want to have the right to have access to everything and want to make sure that the infrastructure is there to do it. From a blindness and vision impairment perspective, when things have been buried in paper, of course there is an inherent barrier there and you're depending on other human beings to read the stuff to you. The promise of – in an electronic age where things can be adapted means that there is an even higher, sort of like the theory of rising expectations. Right, so I think there is a sense that because we're in a digital world and the stuff can be made accessible, it really ought to be. And that means the more material the better.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Mark, you do know that of course there's now great technologies so that if you get copies of digital records, they can be read.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Okay, so I'm going to cut the discussion of this question off and turn to Paul Egerman.

Paul Egerman – Businessman/Software Entrepreneur

Thank you Leslie, actually, seeing that there are fair number of people raising their hands, why don't we go ahead and do Wes Rishel and David McCallie first and then come back to me. I want to make sure they get their questions answered.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Wes is next in the queue. Wes?

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Hi, this is Wes Rishel. We've heard discussion I think on three points as I try to sort it out. One is the patient's right to access about their information, their clinical information, and their financial information, anything that is collected or used by the covered entity. The second thing we've heard about is accounting for disclosures, which is to say giving the patient or the patient's representative access to information every time – access to the fact that information left their organization every time it leaves that organization. So if one member of the workforce of the organization shows it to another one or accesses it in the computer, that's not a disclosure as defined by the law. If they send it to another organization, then that is a disclosure. Then the third thing that has been at le – I think implicitly raised is accounting of access, wanting to know which member of the workforce or all the members of the workforce who accessed my information. I wonder if the speakers could just focus – just tell us – I think we can all stipulate that the patient's right to access the information is paramount, between accounting for disclosures and accounting for access, what are the speaker's positions?

Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator

Wes, this is Joy Pritts and is Linda still on the phone, Linda Sanches? Because there was a statement that you made about disclosures that I don't think was quite 100% accurate.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Okay.

Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator

Linda, are you there? Okay, so the – one of the, it's splitting hairs perhaps, but for example if you are in a hospital and you have a doctor who is on the staff, who is an employee and that doctor opens a record and reads it and looks at it, that is a use. If you have another doctor who is not an employee, but who has privileges there, so he is a distinct covered entity, when that doctor opens that record, that's considered to be a disclosure.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

So, that –

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office for Civil Rights

Hello, this is Linda Sanchez, I'm sorry for the delay in responding, but Joy that was absolutely correct.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Okay, so let's turn to the three panelists and I'll just ask them in order, Mark, Deborah or Michelle, any thoughts on this?

Deborah C. Peel, MD – Founder – Patient Privacy Rights

This is Deborah. Yes, we would – we believe that we should have both uses and disclosures and that there's no need to create a separate process. Part of what we outlined in our paper was a very simple way to do this. Any users or disclosures can be treated in the same way when those – the person that's making the use enters that into the accounting of disclosures log. The patient gets a copy of who that was, why they used it and what the data was. If it's a disclosure, the patient gets a copy of who sent it, who got it, what purpose was and what it was. It should all be automated, using Blue Button Plus, using Direct – the Direct Project and so that if we automate this, then it will be very cheap or cheaper for all of the entities that hold our data and we'll get all the useful data.

And that's the simplest way, not to complicate this any more than it needs to be, because this actually again, it enforces the kind of requirements we've long had to be able to get copies of PHI. It piggybacks on setting up HIE of one, which we very much need, we need alternatives to institutional control of our data and an HIE of one is a perfect way to do it. And patients need to be first-class citizens. So, we should really try to simplify this by using the kinds of technologies that are out there already. Access and authentication logs that know which employees saw the data that know who the recipient is of the data, that kind of thing, who the data's sent to. We should use the existing great security technologies and the new technologies that will allow us, as patients, to be first-class citizens and really profit from our own information.

Michelle de Mooy – Senior Associate, National Priorities – Consumer Action

I think the only thing –

Deborah C. Peel, MD – Founder – Patient Privacy Rights

So – the same – treat it the same, use the technology that's there.

Leslie Francis, JD, PhD – University of Utah School of Medicine – National Committee on Vital and Health Statistics

Mark or Michelle?

Michelle de Mooy – Senior Associate, National Priorities – Consumer Action

Yes, this is Michelle. The only thing I would add to Deb's comments is that from a civil liberties perspective, we think acc – of course we think both access and disclosures, but also government access needs to be included, we think. And like I pointed out about the HIE access points, that has become such a ubiquitous thing in terms of medical data being flown across borders and to different agencies, and we think that's important to be in accountability as well.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Yeah, let me second what she's saying.

Mark D. Richert, Esq. – Director, Public Policy – American Federation for the Blind

This is Mark. The only thing I would add to this, not being anywhere near the expert that my two colleagues on this panel are on this, it seems to me that in a computer rage, I don't know why – presumably someone who accesses this information in either of the two scenarios you put forth, the person on staff or otherwise. They have certain permissions, they have certain authorizations to get in, and presumably they have to proffer those credentials when they try to access the infor – when they try to access a system, etcetera. I'm not sure why it should be so complicated to tag or can follow those tags through, I mean, that's a fairly common thing that we've seen in other areas, it seems to me.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Okay, the next question comes from David McCallie.

David McCallie, Jr., MD – Vice President, Medical Informatics – Cerner Corporation

Yes, hi, it's David McCallie with Cerner. I want to just drill in further on Wes's question and allow for further comment and point out that in a modern automated system, many of the accesses to patient-specific data in the system will not be by humans per se. They will be by automated rule systems that are checking for alertable data, drug interactions, constantly sort of scanning the data. It's an artifact maybe of the paper world where you think of someone opening the chart and it's usually a human who opens the chart in the paper world. But in an automated world, most of the accesses, I suspect in fact, are not specifically tied to a human. And I'm curious to know what are practical boundaries for the kinds of accesses that you've been describing which you have all used a human in the loop, person and human and purpose. What's the boundary between those kinds of accesses and just the actual running of the system, which in fact requires many unattended, nonhuman-mediated accesses to the record, all of which to the computer is the same thing, it's a query against a table.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

– have you got thoughts on that?

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Ah yeah, this is Deborah, as usual, as usual I have thoughts. First of all, some of those automated accesses are for various kinds – like you're pointing out, various kinds of alerts or checking for drug conflicts or whatever they are. I think that those clearly should be reportable too; because patients would be frankly reassured to know the kinds of things like that that the systems are doing to protect them. Part of the problem with those kinds of accesses is sometimes, and I don't know, we should be able to know whether these are uses or whether they're disclosures and to what system or private entity outside of the – let's say the hospital or the doctor's office the data goes. And so, just because actual humans actual data is not transferred person-to-person, you make an excellent point, any time data is transferred automatically for any reason, research or good purposes or reporting purposes for public health and so forth, reporting like Michelle was talking about, we need to know about those things as well. We need to know about them.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Michelle?

Michelle de Mooy – Senior Associate, National Priorities – Consumer Action

Yeah, I think it was a really, really great question. And I think my answer would again parallel Debs. I agree because I understand the point that I think you were sort of trying to make, that listing the hundreds of times perhaps a day that a computer crosschecks something seems tedious. But I do think that there are modern systems that can sort of collate some of that to make it an understandable disclosure I think, otherwise it would be pointless if you're listing all of this sort of jargon access that a computer was doing something that the consumer really doesn't understand, that wouldn't be useful. But if it's disclosed in a way that allows them to understand the point of it, the purpose of it of course, the reason a computer is crosschecking something, and then I think it would make sense to include it each time.

Mark D. Richert, Esq. – Director, Public Policy – American Federation for the Blind

And this is Mark. The only thing I would add to that, again, I don't really – it's funny, I didn't even think about a distinction between human versus an automated thing as I thought about sort of the accessibility angle for this. We kind of run up against this all the time and have with respect to either Section 508 of the Rehab Act and whether or not the federal government's buying accessible technology and the extent to which does that apply? How does the accessibility get impacted when something is automated versus when a human being is involved? And presumably when those queries are made about whether or not there are conflicts in medication, etcetera, presumably that computer has an identity, presumably, I mean the computer's not making the decision on its own, it might not in that individual instance, but certainly it's been authorized by somebody to make that query. So it seems to me there are ways of identifying who it is which entity it is that is seeking information.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

This is Deborah. I can foresee institutions saying, well, it's going to take a lot for us to turn all of these logs and all this computer language into something that patients can understand, human beings can understand. And that might be true that it's difficult, but I can promise you if we get the data and even if it's not humanly readable, an industry will develop to translate that data into meaningful ways we can understand and use it for ourselves. We should have the right to decide whether we like whichever pharmaceutical companies conflict – drug conflict algorithms we like or if we trust someone else's opinions about the drugs we're on, for example. The point really is, in the worst-case scenario, we would take whatever is in the system because if we can get it and collect it, a whole new industry working for patients, working for you and your families will develop to serve us. Because there are plenty of smart people who can figure out how to make sense of that data for the rest of us.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

We have five minutes per person left, because there are five in the queue and 20 minutes. So I'm going to turn now to Peter Kaufman.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Thanks. My question's mostly for Dr. Peel. I went to preface it with a couple of points. First of all, like you I'm a provider and a patient, but I'm also a vendor working for a company that does healthcare interconnectivity and electronic prescribing. And the question is regarding the control of the data map. We've talked about disclosure and access and patient having access to that information, which I agree is the final point we want to get to. Certainly as a provider there have been patients who've accessed their data and had no idea what to do with it, but the questions were generally good ones. And while it took some time, it ended up in the patient's good for the long run. But here we have to remember that perfect is the enemy of good and getting to this is not going to be something we're going to get to immediately.

But in terms of the data map, there are certainly patients who want to control exactly where the data goes and how it's going there. But many patients who were either unable or more commonly, unwilling to control that access, they just – this is something they trust their doctors and they do not have the same kind of interest that you and many other people do. How do you picture that data being controlled for those patients? Do you think of the primary care doctor doing it or do you think of a proxy? How do you picture that happening?

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Well, that's a great question; there are a lot of ways that it could happen. First of all, I think many people don't know that they have the right to control this data and assume, for example, that the doctor or the provider is acting in their best interest and they may not be. So, I think that as people begin to understand what's going on in health technology, most people will want their data. There will arise tools that enable them to use agents actually that work for them, not for large institutions or vendors that will come up to advise them. There will be nonprofit groups like us, like Consumer Action, who can develop default ways to have your information handled and help you make decisions about it.

But for the time being, the people that are not interested, for example elderly people, they may well want a son or a daughter to manage their information for them. So, I think this is going to be a learning process and those that don't want to manage their data now, I think it's not a matter that they don't want it, they just don't know what's going on and they have not had any options. They've had no options whatsoever and so we have a long way to go to educate the public about what's going on with their data, and we're just at the beginning of this. But I think the day will come when people will understand that their health information is the most valuable personal information about them in the digital world and it's an asset, it should be protected in the same way they protect and control their financial assets online.

Michelle de Mooy – Senior Associate, National Priorities – Consumer Action

This is Michelle. Yeah, I just would add, I think sometimes when we would talk about these privacy concerns, there's a tendency to overlook really practical issues and for us, when we're dealing with more vulnerable consumers, that's really how we try to focus some of the solutions. So this is just a minor point, but it's one that I think needs to be made, which is that these disclosures need to be made in multiple languages. I think that is a huge issue that doesn't seem to be something that is addressed often. Also, one of the ways, for example, that we deliver some of our educational work was through wallet cards. We gave consumers in English and in Spanish, questions to ask. So arming people with information isn't necessarily – I think Deb made a good point, just that it's something that is very possible and it just, again the choices need to be there for them to make, to be able to ask the right questions to be able to make the choices.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

I just wanted to reiterate that perfect is the enemy of good. I practice in the Washington, DC area and my patients speak dozens of languages. I agree that this should be something that they can all access and read, but we need to remember to get it done simply first and then expand it to be doing everything over the long run, but not expect everything to happen in the next couple of years.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

This is Deborah. I just wanted to add one thing that I forgot to mention about the question of machine access and automated access. I think the simplest way to think about that is anything that's in a security log, we want it. If machine access is not logged in the security log, don't worry about it; if it is, we want it. And I think that's the way to get to the meaningful machine use of data, personal data.

David McCallie, Jr., MD – Vice President, Medical Informatics – Cerner Corporation

Could you – this is David. Since that was a follow up on my question somewhat, could you qualify what you think a security log has in it or why something would be in a security log?

Deborah C. Peel, MD – Founder – Patient Privacy Rights

My understanding of a security log is it's about the people that are – it's about authentication and it's about where the data goes, for example is about breaches, watching for breaches so, that kind of thing. There are a lot of security products out there I think that try to catch breaches or have algorithms to catch breaches for example, that would be the kind of thing where information is potentially being risked – being put at risk for use that we would want to know about.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Okay. The next question comes from Walter Suarez.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

Yes. can you hear me?

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Yes.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

Okay. Yeah, thank you. I think there continues to be in my mind a little bit of a mix between access, use and disclosure of data to the patient for the patient's certainly ability to have that data and use it and give it to others. And then the concepts around documenting and reporting to the patient details about the disclosure of that data to others or who has used the data inside an organization. And I wanted to bring it back to really sort of a point of trust and balance in many respects, and I wanted to hear the reaction of the testifiers on that point. Because in some ways, when you think of a patient going to a clinic, even before the patient goes to the clinic, they make an appointment, they contact the clinic, do the processing of that, the clinic then does some processing before the patient comes in. Then the patient comes and then after the patient leaves there is some more activity. And one can see the number of instances, or can think about the number of instances that inside that clinic, different people had to access and to use the record for different purposes. And in most cases, basically the expectation from the patient would be that the individuals inside that organization will be accessing and using the data so that they can treat them better.

And so in some respect, there is some level of expectation of the patient that these types of uses are going to happen.

And so when one thinks about reporting the back after the patient has seen several doctors and several encounters back to the consumer, of all the instances. And again, one can imagine the many, many different instances of accesses by virtue of using the data of employees and individuals within an organization, it becomes such a voluminous amount of information that it begins to break the fabric of really trust between the patient and the provider for treatment of that patient. And it creates an issue of balancing the ability of providing better care to the patient with having to create systems and maintain documents and then report out information the consumer that the consumer will find in many cases probably confusing. So the question is really about trust and balance and to what extent some of this expectations of yeah, I want to see every piece of information – (Indiscernible), every piece of information that anybody has seen for what purpose, when and why and how and balancing that with the trust that a patient puts on the provider to use that information.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Well Walter, this is Deborah. I think you've got the trust exactly backwards. You seem to be saying that if people actually knew how many different people used parts of their data or looked at it or disclosed it, they wouldn't trust their doctors? I think that's backwards. I think the only way that they can trust the doctor or the system is by knowing what's going on. Hiding who has access and what it's for, doesn't generate trust. That's really the whole point of complete reporting. And yes, we understand it will be voluminous, but when we have this voluminous data, again, there will be wonderful people that develop apps to make sense out of it for us and so we can use the data for own benefits and to understand better what goes on in healthcare.

I mean, I guess if someone's office had I don't know, dozens of nurses looking at one patient's records, they might get scared or not trust the doctor. But that could lead to an important discussion about why so many nurses or so many technicians or so many back office people or whatever were looking at the data. These are important things to know with the incredible risks of medical identity theft and identity thefts that go on right now. And certainly systems with thousands and thousands of employees that can access millions of people's data, create tremendous problems with trust. The trust problem exists now.

Mark D. Richert, Esq. – Director, Public Policy – American Federation for the Blind

This is Mark. I mean – I'm just not sure that we – it's just sort of like in the credit reporting area, I'm not sure that the fact that there are credit reporting agencies makes people feel less confident or trusting of the banks that they use or their own creditors. I think the point is, we have reporting in those areas so that we know if it's somebody other than those that we have access to. And I also don't think that anybody should ever feel, I mean I'm not suggesting what's the line, if you didn't do anything wrong, you don't have anything to worry about when the police question you. It's not so much that, but clearly if everyone is operating aboveboard, then there should be no one who should be spooked by reporting and accountability.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Michelle? Do you want to chime in Michelle?

Michelle de Mooy – Senior Associate, National Priorities – Consumer Action

I have nothing to add.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Next – on the line?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Thanks Leslie, I know Judy was trying to get in to the question queue, too. I'm willing to defer being one of those people not online.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

I know Dixie Baker is not on the web but would like to ask a question.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates

Yes, thank you Leslie, I appreciate that. First of all, I want to thank the panelists for your very, very useful testimony there. We – both in the testimonies and in the question period we've talked about what information should be available and to whom, whether the disclosures are to humans or to software. But it seems – we have seemed to have focus on identity and not on how much context information a patient might need, for example, the role that the person has and the purpose of the access or the use. And many of the identities will not be known to the patients, so I'd be interested in hearing your thoughts on what information needs to be provided, in addition to identity, to establish the context for a reported access or use, so that the patient will understand why that reported use or disclosure was made.

Leslie Francis, JD, PhD – University of Utah School of Medicine – National Committee on Vital and Health Statistics

Panelists?

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Sure, this is Deborah. We and actually, we worked with Consumer Action and Michelle's group and others, we all believed that the role and the purpose needed to be in that to help establish the context. We – so that's why that was there. Yes, we think context is very helpful. Part of why I've said it's critical to get the logs with whatever is in there to us, even if that is not part of it, is because we believe that once we have that information, we'll find ways for some of that to be worked out and presented to the patients. For example, if we get a log that doesn't have a purpose and has the name of the person and that's compared with let's say a list of employees and their job titles, etcetera, some of that could be inferred. But yes, context is important but at the very least we need, if institutions are going to argue that that's too hard or too difficult a step, we want the data that's there.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Michelle or Mark?

Michelle de Mooy – Senior Associate, National Priorities – Consumer Action

I would just briefly echo what Deb had said, that I think yes, context is important. And from my perspective, everything that is possible to make the disclosures readable and understandable and actionable by consumers should be there. And context would of course include the role of the individual or the purpose of the computer crosschecking, the day, the time, I think all of those things lend to making these disclosures actually actionable and useful to people.

Mark D. Richert, Esq. – Director, Public Policy – American Federation for the Blind

This is Mark. The only thing I would add is, as someone who works in the world where there are these fun things called meta-tags that are used to provide text labels for things that are coded on a webpage, for example. These ALT tags, I think, are the kind of things that I'm sure there's an analogy to it in this world where things that otherwise are pretty unintelligible to the layperson can be tagged with things that are more intelligible. That obviously takes some time, and I suspect that probably you all will say we're probably at the relative infancy of making that happen. The only thing I would say is that at an absolute minimum, even if the typical person isn't going to be able to intelligibly translate a series of numbers or codes, at an absolute minimum making sure that that information is available to someone or something that can interpret that information is the key. I mean, I don't think anyone is going to be sitting around in between watching soap operas, going up to look at their health records. I mean, I think what it boils down to is they want that the information available to them when there's a reason to check. And if that means that the information isn't exactly going to be in narrative or even poetic form, but it's in some form that's at least a) complete and b) can be understood by somebody, that's really where the action's at.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Is there anyone else on the phone with a question?

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation

Yeah, this Judy.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Okay Judy, there you go.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation

Yeah, two things. One, I don't know how to handle the employed docs versus the unemployed docs because in some states, for example California, the hospital is not allowed to employ doctors, they are always separate. So that dividing it between employed and unemployed docs may be a problem, that's one. And the second is a comment. I'm certain about the comment that your doctor might not always be doing thgs in your interest. I just wanted to say most of the doctors, huge proportion of them, are wonderful, dedicated, caring and concerned about their patients and those who are not are the great exception and in no way the norm.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Judy, as a physician, I absolutely agree with you. But today, our physicians cannot prevent our data from being blown around the world because electronic health records, like yours, don't permit patients to control any of the uses or disclosures.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation

I was just commenting on –

Deborah C. Peel, MD – Founder – Patient Privacy Rights

The doctors can't help us or protect us, and they want to.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation

Yeah, and that's what I agree with Deborah, the comment made earlier was that they may not be acting in your best interest and I wanted to make a comment about that, because I don't think it's accurate for the most part.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Well, for example, if your doctor chooses an EHR that sells the data, and that's up front about their business model, I think you'd agree that at the very least, that particular choice puts patients at risk of harm and is in the doctor's interest, of making more money, but it's not clear how much that serves the patients.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Michelle or Mark?

Mark D. Richert, Esq. – Director, Public Policy – American Federation for the Blind

I think there are some times, and I'm not going to belabor how – the hypotheticals. But we can all imagine situations where someone thinks that they're acting in someone's best interest by passing along information. And the truth is that the recipient takes the information in a different fashion. The disclosure, for example, that someone has a certain medical condition, the fact that for insurance purposes or coverage purposes. Even though we all know that there should be reasons why that – today, why that shouldn't be permitted to be used in a discriminatory fashion, I don't think we need to worry about the motive necessarily of the person who's using it. It's about documenting who has had access to what so that in the event that something goes awry, we can track it and trace and figure out what the heck's going on and hopefully address it in the future. I don't think we need to get into what – are these good people who are playing with this information it really doesn't matter.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Michelle?

Michelle de Mooy – Senior Associate, National Priorities – Consumer Action

I have nothing to add.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

I think the next question is from Paul Egerman. Paul, I put you on – no, you kind of deferred and now it's your turn.

Paul Egerman – Businessman/Software Entrepreneur

Yeah, I want to ask – we only have a short amount of time because we have to get started on the next panel, but a lot of the –

Leslie Francis, JD, PhD – University of Utah School of Medicine – National Committee on Vital and Health Statistics

That doesn't start until 11 – til 1:15, so –

Paul Eggerman – Businessman/Software Entrepreneur

Okay. A lot of the comments are sort of predicated on the idea that the security logs is where information resides and valuable information can be obtained. But there may be many physicians who access the data and simply aren't listed in the security logs, for example, a surgeon who performs the surgery, may have access to all kinds of information in the operating room, certainly access to the patient, but does not appear in the security log. Similarly, radiologists might not be in the security logs. A lot of people who touch the patient, like a phlebotomist, might not be in the security log, even though they have access to the data because the data is presented to them, is pushed to them. And so my question is, how does that influence the usability of the security logs if key clinical people, key physicians aren't listed in an access report?

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Okay, yeah, this is Deborah. I might not be accurately – I might have been misunderstood. I think whatever is reported in a security log, those kinds of uses and disclosures need to be reported to us. But, when a surgeon goes into someone's record in the operating room that is certainly logged in –

Paul Eggerman – Businessman/Software Entrepreneur

Not – Deborah, not necessarily, I mean, not necessarily. You're assuming a surgeon is going to login, it could be a resident logs in for the surgeon who prepares the information for him or her and the surgeon never touches the computer, because a surgeon doesn't want to touch the computer.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Yeah, I hear you, that's a whole other kind of problem that I think medical records are not yet up to speed with, one person logging in for another and hopefully there's some way to correct that so that could be resident "X" is signed in for doctor "Y," so that there would be some idea –

Paul Eggerman – Businessman/Software Entrepreneur

I'm sorry, you're not – you don't understand, a surgeon could walk into an operating room and have somebody already present to him on a screen, like a CT scan, information for the patient. And it's not like they're logging in instead of him, they're just logging in for everybody in the operating room and so the information is visible, it's sort of pushed to the surgeon. But the surgeon might never login himself and nobody's really logging in for the surgeon, it's just the information is presented to him or her.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Well, but you see what I am saying, when someone's facilitating a treating physician with their work, there probably needs to be better ways to indicate what's really going on so that we know. I mean, it would be shocking to get a hospital record where you had surgery performed and there were no logs of your surgeon getting into your record. People would wonder who – what's that about? So I think this just has to do with not having figured out how to accurately represent who's doing what and because access is been so difficult, people used to leave the data stations open under other people's name and login and do stuff, and not even under their own name. But all that stuff has to get sharper and better because it doesn't accurately reflect what's going on. The point is to accurately reflect who's using and seeing the data and the systems aren't really up to speed yet.

Mark D. Richert, Esq. – Director, Public Policy – American Federation for the Blind

This is Mark. I mean, I don't know if my other panelists are going to throw mud at me for this, but honestly, I'm not so much worried about – I mean, everybody has a secretary. I think we can understand those situations where, my God, someone else has logged in for me and it just is someone who really isn't the person sitting at the terminal punching in the password, are they getting information? That's going to happen so long as you don't have a mechanism for absolutely proving that the person who's typing it in is the real person. That's – it's of concern but for my money, the biggest concern is to have access to – whoever it is who is ultimately accountable for the information.

So even in the situation that you're describing, the operating room, things are happening quickly, somebody somewhere has logged into the system, even if it is a corporate entity Holy Cross Hospital that is the one that is essentially displaying the record. If we know that, then at least we have some place to go in the event that information has been shared inappropriately. I mean, I think that's really the issue, not were there four, five or six human beings who happened to look at the screen or happened to get information. I mean the fact that an individual may have information that they shouldn't have or that the patient may not want isn't really as important as the ultimate accountability for that information and frankly, getting made whole in the event that something goes wrong with that information.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Well sure, but what you're talking about is actually not accountability, because I've seen some really great systems, actually one that was designed for EPIC records where every person has a card and the card recognizes it's you, when go in a room, pops open the screen for you and that patient, because you're connected. When you leave, it shuts down, when you go the next – I mean, there are much better systems for logging people in and out of records and I have seen some of them, and that's the future. Because there is an accountability if you don't actually know who's seen it and that – again the reason for needing to know this is the data's so valuable and so many low-level employees are – frankly are stealing data.

Mark D. Richert, Esq. – Director, Public Policy – American Federation for the Blind

I would just say –

Leslie Francis, JD, PhD – University of Utah School of Medicine – National Committee on Vital and Health Statistics

Sorry to interrupt –

Mark D. Richert, Esq. – Director, Public Policy – American Federation for the Blind

I don't disagree with that, the only thing I would say is that the low-level employee is probably – you're not going to be able to squeeze a lot of blood out of that turnip. If there is some financial or some other issue that has taken place, that low-level employee is not going to be the one you're not going to go after. You're going to want to go after someone who actually had serious responsibility for that information – you're not going to get much remedy out of that.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

– I need to ask Michelle if she has a last comment because the next panel is supposed to go in four minutes. And Wes, I'm sorry I didn't have a chance to get back to you for a follow up.

Michelle de Mooy – Senior Associate, National Priorities – Consumer Action

Sure. Yeah, hi, this is Michelle. I would just comment that this is sort of one of those intersections between human beings and technology that I think is a tricky question. But I think when it comes down to the technological system you have, making sure that it provides enough clarity for the people using it so that they're able to accurately document what is occurring, and it's not to be ridiculous, of course. Right, if somebody – if you start to look at gray areas where somebody's looking at something or not, then you get into the issue of – training. And that – it continues to be of utmost importance, so people are starting from a patient privacy perspective.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Well thank you very much for the panel on the patient's perspective and for a wonderful discussion from everybody. And I look forward to the rest of the virtual hearing.

Paul Egerman – Businessman/Software Entrepreneur

Great, thank you very much –

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Leslie, I can make my statement in less than a minute.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Pardon?

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Leslie, this is Wes Rishel, I can make my statement in less than a minute.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Okay, go for it.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Okay, so I'm concerned that on the one hand I hear people implying this is really easy, it all relies on existing technology and then upon being challenged, start talking about completely refitting all systems for the way they authenticate users and the workflows that they use. I'm also concerned that we're not talking about a single system, the EHR and – medical center, under the proposed rule, it was electronic designated record sets, which represent 100 to 150 different systems that need remediation. Thank you.

Paul Egerman – Businessman/Software Entrepreneur

Thank you very much, Wes. Paul Egerman, and actually your comment is a good segue to our next panel. Our next panel is a group of vendors. We have four vendors who are going to address the technical feasibility of accomplishing what has been suggested, analyzing logs and producing access and disclosure reports. And I want to start out by thanking each of these four people for participating in our hearing. I know we gave you very short notice, I also know for vendors September 30, the last day of a quarter can sometimes be an exciting day and so I appreciate your participation.

And in case you did not hear Deven's initial comments to the prior panel, we are limiting very carefully and rigidly, without mercy, holding everyone to a five-minute limit. And we are doing that in your presentations because we are simply trying to be fair to the other presenters and to the people on the telephone. It's difficult to do this over the telephone because we don't really want to stop you, we very much value your participation. So we hope that we're not forced to stop you but at four minutes and 30 seconds into your presentation, you will hear a warning signal, which apparently is a rooster. I cannot tell you why we use a rooster at the end of four minutes 30 seconds except it is not like evidence-based hearings, it's just something that we do and it works. I suppose that's the way healthcare works sometimes also.

So having made all these comments, our first presenter, and again, I just want to say thank you to all four of these people, it's really terrific that you are here, I feel like I'm not doing you justice with my very brief and terse introduction of each individual and each company. But first, we have Kurt Long, who's CEO and Founder of FairWarning. Kurt, are you there?

Kurt Long, MS – Founder and Chief Operating Officer – FairWarning, Inc.

I'm here.

Paul Egerman – Businessman/Software Entrepreneur

Terrific.

Kurt Long, MS – Founder and Chief Operating Officer – FairWarning, Inc.

Are we all set?

Paul Egerman – Businessman/Software Entrepreneur

You are all set.

Kurt Long, MS – Founder and Chief Operating Officer – FairWarning, Inc.

FairWarning has focused exclusively on healthcare access reporting and user activity monitoring since 2005. Our expertise and testimony is focused on the value of access reports in general and the practicality of generating patient-facing access reports specifically today. Beginning in 2005 through the present, the first use case required by our customers has always been to support a simple internal use access report. Simple access reports are in use by customers representing 1100 hospitals and 4000 clinics and facilities throughout the United States, Canada, the United Kingdom and Europe. About 85% of these are in the United States. An internal use access report details access to a given patient's records across all applications used in healthcare treatment, payment and operations, usually over a specific date range. It includes date and time of access, user name and identifier as well as department of those who accessed. Patient name and identifier, function and purpose of access, many other details may be included such as facility, floor, bed as well as descriptive detail of access. However, the availability of these details and the formats of access logs vary dramatically between the applications used in healthcare.

Common care provider uses of internal access reports include: investigation of a patient complaint brought directly to the care provider, investigation of a patient complaint directed through HHS, response to an external legal discovery, forensics research in support of information security investigations, investigation of a patient access as part of a health information exchange. Legal documentation for defense against civil lawsuits such as unlawful termination, which are routinely brought against care providers, and increasingly supportive law enforcement investigations, particularly cases involving the theft of patient identities for use in false IRS tax returns as well as medical identity theft. While the ability to conduct a simple access report and associated user activity monitoring is invaluable.

Access report, as defined in the proposed rule, is technically infeasible due to the lack of widespread availability and detail contained in access logs produced by application vendors. Further, the proposed rule, to be practical, would need to have a highly simplified patient-facing format, which would be easy to read and understand. In our opinion, the FairWarning – the proposed rule as written would have a large untold burden to care providers in explaining each and every access by every care worker and an overly detailed access report would create patient confusion and stress, unnecessarily injuring patient trust in electronic health records.

FairWarning has examined and documented access logs generated by 519 applications used in healthcare and when versions are considered, the number grows to nearly 1000. I'll summarize our findings over the past eight years, and first the good news. Since 2009, we have documented an increase of applications routinely supporting access logs growing from 60 to well in excess of 200 today. Every major electronic health record vendor with considerable market share produces an access log that care providers can use to produce an internal use access report. Meaningful use criteria requiring electronic health record vendors to include activated access logs by default has greatly improved the consistency, availability and robustness of access logs for meaningful use certified technology.

For applications that are not subject to meaningful use criteria, nearly 50% of the 519 that we've examined or nearly 250, do produce an audit log that's suitable for the production of an internal use access report. The Office for Civil Rights HIPAA audits in definition of user activity monitoring in their audit protocol has heightened care provider's attention to the need for the centralization and use of access logs for compliance, privacy and security. The net effect on application vendors who serve those healthcare providers is they are beginning to embrace the need to deliver basic security features such as access logs at no charge and by default. Care providers attesting for meaningful use are giving far more attention to the privacy, information security and HIPAA Compliance Programs than in the past. With current government – current and pending governmental audit programs serving as highly motivating factors, we believe the permanent HIPAA Audit Program is essential to transitioning from attention to privacy, security and compliance to actually investing in privacy, security and compliance at a large-scale.

These positive trends, however – are positive trends; however, there's considerable improvements in order to make the access report, as defined in the proposed rule, feasible. Over 250 of the 519 application access logs examined do not routinely produced an audit log. We've seen vendors attempt to charge as much as \$20,000 to activate an access log and in general our going forward recommendations are to build on the successful work of the ONC in requiring certified EHR vendors to produce an access log by default and extend the requirement to all application vendors who serve healthcare. There needs to be a robust, ubiquitous and practical standard for the contents and production of access logs in a dramatically simplified patient-facing format for the access report. Thank you.

Paul Egerman – Businessman/Software Entrepreneur

Thank you Kurt. Thank you, very useful information from somebody who's got a lot of experience looking at these security logs. Next we have Eric Cooper, who is the Health Information and Identity Management Product Lead, that's a long title, for EPIC. Eric, are you there?

Eric Cooper – Group Lead, Software Development – EPIC Systems, Inc.

I am. Good afternoon. As you mentioned, my name is Eric Cooper and I'm a software developer here at EPIC. My primary focus is on health information and identity management. That area does include our technology to cover access logs as well as disclosure modules and disclosure within the system. I'd like to first thank the committee for inviting us to comment on this topic and I will like to focus my testimony on two of the committee's questions that were directed at vendors. First you ask, what are software's current capabilities around access and disclosure of PHIR? As our software contains access logging for both clinical and nonclinical workflows, as well as an integrated module for capturing and recording on disclosures, the software is designed to deliver accesses of patient information are logged and recorded on. Health information professionals use the access log to perform audits and investigations and as such, it is formatted for a quick review.

The data log is typically the user, patient, date, time and type of information used. For example, if the nurse logs into the system to room a patient for an ambulatory visit, the nurse will open the patient's record, review their meds, their allergies and record some basic vitals. And then typically document the chief complaint for the visit. They will then log out. This simple workflow can result in 20-30 entries in an access log. This actual 20-30 entries in that access log can be compounded by the fact that the number of users that typically access a record within one visit and one episode of patient care. In an ambulatory setting you can have 10 or more users typically accessing the record throughout that visit, and each one of those will result in hundreds of entries into the access log.

If you then go to an inpatient visit, the number will quickly balloon, you typically will have 30 plus users, and if it's a long stay, you may have more and more as the shifts change and different nurses and users log into the system. This will result in easily thousands of entries into that access log for that single episode of care. And we did test it myself this morning. I did log in and within one minute of a workflow, typically performing what an end-user would, it resulted in 35 access log entries. The log is intended to allow for a detailed analysis. The format and detail would typically not be easily decipherable by a patient unfamiliar with the system. It would likely take the security professional a significant amount of time to walk the patient through the access log, to make sure that they can understand it, especially if it's containing the past three years' worth of data. We think that it might likely take much longer than performing a target investigation to meet that patient's needs.

Also note that logging of delivered access currently results in massive amounts of data and subsequently hard drive storage, typically taking up more than 50% of an organization's reporting database, which also contains all clinical and financial data, obviously adding a great deal of data storage and cost for that storage for organizations using an EHR. When discussing access logs, it is important to note the different types of EHR data access that can occur. The examples I've given so far are all deliberate accesses to a patient record. There are also many workflows where user maintenance can definitely see a small amount of information from many patients on a list, such as a report or the scheduled for the day. A nurse reviewing the schedule of patients with visits that day will see a small amount of data for each one. She may only access one of those patients from the list and the nurse's actions, when they do look at it, is tracked. We do track that they look at that actual schedule, we only give nurses appropriate schedules to view, so the tracking is at the level of the nurse, not the level of each patient displayed on that schedule, unless they enter it to take further action and review that record.

The next question I would like to address is whether the software captures purpose along with every user access to the patient's chart? The software currently does not capture a purpose as the user enters different patient records throughout the day to complete their work. To properly address this question, to contemplating what it might take to capture purpose on general workflow actions that expose patient data. We initially thought maybe we could infer purpose, based off of the user's role and the type of data that they're looking at. For example, let's consider a physician workflow. Dr. Smith would access the patient record to review a new lab result. It might be reasonable to infer that that access by a clinician to a lab result is for treatment. However, Dr. Smith might also access similar data to perform peer review in another physician's work, or while monitoring the overall quality of their clinic. So perhaps it's not quite as accurate to infer that all of those accesses are for treatment.

So in summary, since I have only 30 seconds left, multiple healthcare organizations have informed us that patients rarely, if ever, request an accounting of disclosures. Most requests are related to suspicions of a particular person, such as an ex-spouse, has accessed their record inappropriately. These requests are better served by having a health information professional perform a targeted investigation, rather than handing the patient a report containing thousands of accesses from the previous three years. For these reasons, users of our software tell us that requiring provision of an access log report to patients is not the best path. I would also like to urge that as future uses of the access log are considered, that the workflow cost of gathering data and the technical and storage costs of retaining such are balanced with the value the data will provide. Thank you for your consideration.

Paul Egerman – Businessman/Software Entrepreneur

Thank you very much. Excellent presentation and extremely helpful. Next we have Jeremy Delinsky, who's the Chief Technical Officer of athenahealth and also Stephanie Zaremba, I sure hope I pronounced your name correctly Stephanie, Senior Manager of Government and Regulatory Affairs, athenahealth, are you there?

Jeremy Delinsky, MBA – Senior Vice President, Chief Technical Officer – athenahealth, Inc.

We are here. Thank you. Good afternoon, thanks for having us. I apologize in advance for my voice, I'm starting to lose it. But again, my name is Jeremy Delinsky and I'm the Chief Technology Officer at athenahealth. Athenahealth provides EHR and related services to over 40,000 healthcare professionals in every state. We serve organizations of every size from thousands of solo practitioners to some of the very largest health systems. All of our providers access our services on the same instance of a continually updated Cloud-based software model. We agree that a practical approach to providing patients with greater transparency about the uses and disclosures of their digital identifiable health information is a necessary step toward greater patient engagement.

We disagree, however, that transparency for transparency sake is necessarily a desired outcome. Members of the Tiger Team as well as the broader policy community should begin by addressing a crucial threshold question, will providing patients with accountings of disclosures mitigate the risk of improper access, use and disclosure of PHI in the age of digitized health information? Based on our experience responding to patient inquiries, we believe that patients do not want nor are they well served by an exhaustive accounting of all access, uses or disclosures. Effective transparency of use and disclosure information must be meaningful to the patient audience. Inclusion of all uses and disclosures related to treatment, payment and healthcare operations will not result in transparency, it will overburden patients with business processes that they may not understand and more importantly, will potentially bury the information that the patient actually sought.

It is extremely important to understand the volume of information that would be included if an accounting of disclosures report for a typical patient contained every access, use or disclosure of PHI. The volume is staggering. A typical patient visit will produce between 500 to 1000 auditable events in the provider's clinical systems. Specific views, modifications, transactions with the outside world, new entries related to the clinical and administrative workflows that will require full accounting and declaration of intent. The magnitude and granularity of this information would overwhelm most patients, obscuring instead of revealing any instance of improper access. Further, patient demand for comprehensive accounting of disclosures is low. We've received fewer than five such requests in the past seven years. Rarely patients do ask for specific information about whether an individual known to them has viewed or modified their health information. These specific concerns can best be addressed by more specialized reporting.

Given this low demand, athenahealth's current process for delivering a comprehensive solution would be largely manual. An engineer will say that anything is possible, the issue we're talking about here is one of opportunity cost. It would be a substantial development project, probably in the thousands of developer hours, to create an on-demand patient access review toolset that actually was user friendly for patients. This kind of project would compete directly with work our clients are asking us to deliver that enables higher quality care at a lower cost. We would prefer to spend our resources on activities that have a clear patient benefit.

Transparency will not be improved by attempting to track the purpose behind each use, access and disclosure. Tracking the purpose behind each clinical decision would be difficult to standardize. To accurately identify purpose would require providers and administrative staff to take additional steps to explain their reasons at every step in the caregiving and billing processes. This is unlikely to provide complete transparency, especially because the process would be controlled by those who may be behaving improperly. Another approach would be to develop vendor automated logic based on a set of inferences about the purpose behind each action taken. Such logic could be inaccurate, however, as the inferences would be based on expected and compliant workflows rather than suspicious behavior and such misinformation would be forwarded to the patient in an accounting of disclosures.

It is important that we continue to prioritize transparency for patients among the many Health IT policy objectives. But it is equally important that we do so in a well-planned and intelligent way that augments rather than detracts from the many other important Health IT and health reform goals and that provides useful access for patients to meaningful information. This objective cannot be met if they are provided with indecipherable audit logs of thousands of minor demographic edits, claim follow ups, provider reviews and similar routine, necessary and proper instances of data access. Thank you very much for the opportunity to engage in this important topic.

Paul Egerman – Businessman/Software Entrepreneur

Great. Thank you very much Jeremy and very appreciate your presentation, I particularly appreciate that you completed it shorter than the five minutes. Anybody who completes it in less than five minutes I view as an absolute paragon of virtue.

Jeremy Delinsky, MBA – Senior Vice President, Chief Technical Officer – athenahealth, Inc.

We try, thank you.

Paul Egerman – Businessman/Software Entrepreneur

I really very much appreciate those comments.

John Houston, JD – Vice President – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Paul, you need to crow like a rooster now.

Paul Egerman – Businessman/Software Entrepreneur

Ah, okay. Our final presenter is from Cerner, we have John Travis, who is the Senior Director of Regulatory Compliance and assisted by Lori Cross, Director of Laboratory Operations. John and Lori, are you there?

Lori Cross – Director of Laboratory Operations - Cerner

Yes, we are.

Paul Egerman – Businessman/Software Entrepreneur

Terrific, please proceed.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Is John maybe not on or on the public line?

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

Oh, I'm sorry. I'm on, I'm on, I was muted. Sorry Paul, I'm talking and Lori's –

Paul Egerman – Businessman/Software Entrepreneur

That's okay, we will not charge you for that time.

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

Ah, we thank you. I want my virtue intact. Okay, we were asked to speak particularly to the perspective of an ancillary system participating in the whole matter of the patient right to an access report and an accounting of disclosures. One thing to keep in mind with ancillary systems is that they both can be the main clinical system in a provider setting, like a reference lab or a diagnostic imaging center as well as a participant in obviously a much larger hospital or health system entity.

The first question we really decided to respond to was the one about what kinds logging might be available as a current capability. And with a lab or a radiology system, particularly true of the lab, there could be a number of candidate logs. In addition to the security audit logs that have been spoken of before, there are going to be distribution logs of diagnostic test reports that are a lot of the kind of the normal mode of treatment related disclosures that happen for reporting out the test results. There can be interface transaction logs, both with medical devices as well as between applications, especially in a hospital environment, to report out lab results to other systems, to make them available to the care team.

And then there can be public health submission logs and files that go with reportable lab results and syndromic data that may come out of especially the lab side of things. So aside from security logs, these log sources don't typically provide patient-specific reporting, even though they may have patient specific information in them. And one point that we haven't heard raised really yet, and I'll be able to compliment the other presenters, there's a lot of post-processing that would have to be done to make use of this information, and I'll get to that specifically in some of the next questions.

The question that we also wanted to respond to was the means to distinguish internal use from external disclosure. As others have stated, those can both involve online access so unless there has been specific design for things like user identity or name or user roles, it's going to be very difficult to tell the difference between an employed staff member and a contract person working in a similar role. Secondary metadata about the access that established where the user accessed from might be useful, but often times those individual could be working almost side-by-side. So they can share similar roles, they can have similar access rights and unless there's been a very conscious decision to design those factors in to some of the key security metadata, it's going to be very hard to tell use from disclosure.

Another question we were asked was, uses or accessed that do not raise privacy concerns. A fair amount of conversation has gone on about the volume of access data that may be exposed to the patient. One thing that we do believe needs to be given consideration is how much towards what really are machine operations is relevant to this kind of reporting. The OCR in their proposed rule certainly seemed to have the regulatory intent that machine operations, it could be server to server or machine entity to machine entity could qualify. And the volume of data and volume of login events just goes up exponentially when you consider medical device interfaces, telemetry and things that are common for diagnostic testing in lab or radiology.

If the goal is to hold the provider accountable about internal propagation of the ePHI, we think natural human end-user accesses can account for that, as other presenters have made, most every system should have an ability to provide for access audit logging. And the OCR could identify the system where the access occurred, in the access report requirements if the concern is where did my data go? From a login and retention standpoint, security audit logs likely have the ability to meet the three-year look back, but most of the other kinds of logs I mentioned would require some kind of data extraction and retention outside the source logging mechanism and the post-processing to make any real use of that. And that would be where the manual labor and the very intensive process, I believe athenahealth did a very good job painting the picture of that, would really come into play, if you're going to make use of those kinds of logs.

We also commented on the question of concerns with disclosing names of individuals accessing ePHI. Really aside from sensitivity about disclosing the names of individual staff members, we think there should be a lot of thought given to the difficulties in normalizing user name and identity references across all log sources, particularly when you're thinking of ancillary systems that may not have been implemented in any normalized way. Purpose of use or purpose of access in an understandable manner is also going to be most often implied. We don't believe it's realistic that you would ask medical technologists and pathologists why are you performing that result. Why are you verifying that PAP smear? So distinguishing for the patient what is perfectly normal from what may be abnormal is going to be very challenging if you're looking at a direct implication of purpose of use beyond a general inference of treatment.

So finally, some key summary points. We do recommend that this be an area for best practice or recommended practice guidance in how to normalize data from disparate sources. To really focus on what are the data columns of true value to the end-user, to consider strongly not requiring the reporting on machine accesses that may be between ancillary users and test instruments and things of that nature. And really consider what the post-processing burden is going to look like to come up with a consolidated reporting to the patient that all these systems need to contribute to. And with that I'll be happy to participate in the Q&A.

Paul Egerman – Businessman/Software Entrepreneur

Great. Thank you very much John, and thank you to all four of the presenters who presented from different perspectives. We heard from Kurt Long, who has experience with the security logs. And then we heard from three EHR vendors and exactly as John suggested, we of course know that Cerner provides a complete EHR, but we asked him to present from the viewpoint of an ancillary systems, mainly because we wanted to make sure we had that view point included. So, I appreciate that you did that. And we are now open to questions, and the first question comes from David McCallie.

David McCallie, Jr., MD – Vice President, Medical Informatics – Cerner Corporation

Thanks Paul and thanks for the panelists, very good counterbalancing testimony from our first panel where the request was for everything, all access, regardless. Your group, each of you in your own way pointed out the complexities, costs and perhaps counterintuitive downside of providing too much data that would obscure the important information in the noise. So my question is, are any of you aware of a process that could help us define a middle ground in this space? Or do you have thoughts about how we could define what makes common sense as an approach for measuring what would be relevant to provide to the patient for these logs? I noted John, you used a phrase, natural human access and the phrase, where did my data go? Those two to me make intuitive sense, but what's the process that we can get to a more concrete definition of a notion like that? And it's open to any of you for comment

Kurt Long, MS – Founder and Chief Operating Officer – FairWarning, Inc.

This is Kurt Long from FairWarning. Just a simple observation is to directly involve well-minded care providers that actually have to perform the function that would be required in one of these reports and literally work with them in a roundtable to say what would be acceptable. But I think you need a little bit more care provider input into what's feasible in terms of the data and what they would have to go through in supporting it and listen carefully to what'd have to support in speaking with patients .

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

David, this is John. One thing that I'll observe as well, I think certainly FairWarning I think would have good perspective on this too. The challenge of pulling together logs from multiple source systems just invites, by its very nature, a whole process of how do you normalize usernames, IDs, roles, etcetera in an environment whereby you've got to assume by default they have not been normalized because the systems have been implemented over years and the portfolio at hand is whatever it is. So there's a reason that the patient right has, I think if I remember right, a 30-day response time. This may be more a process than it is a big central logging capacity in the sky maintained on an ongoing basis.

Athenahealth observed that there were only very few patient accounting of disclosure requests over the last number of years since the original HIPAA Privacy Right was there, and I really don't know that the business case is yet well established to create that kind of a mechanism as much as it is a procedure. And I think from my experience, most organizations are really trying to have a response procedure to know where their log data lives and how to compile it, just for the current definition of the accounting of disclosures, and probably would start there for figuring out something like this. But the much more challenging things to go with this really are establishing normalized references for common metadata that have to be part of that access report. And it invites a post-processing to occur.

Kurt Long, MS – Founder and Chief Operating Officer – FairWarning, Inc.

And this is Kurt again and I think you partially invited me to comment. But yeah, I would agree, John. And the way that we've addressed that is we've produced a data definition guide that considers the audit logs, or what I call the access logs. It also considers what we call authoritative user data, which gets at the heart of what you've rightfully identified as a challenge, which is knowing the precise identities of the internal users across all systems. And then thirdly, what we use is another component called advanced patient information. And we combine those three elements, the access logs, identity information together with patient information to produce the access reports that I referred to as I described the internal use. And you're right, it's a bit of work.

Jeremy Delinsky, MBA – Senior Vice President, Chief Technical Officer – athenahealth, Inc.

And this is Jeremy. I think if any of you have ever asked a developer to build a report for you, or if you've ever don't that for somebody, I think what you find is if you ask for all, you tend to get a really bad report back. And so we can all produce reports that show some version of our audit logs, but I think what was missing for me is really getting to the core of what people are worried about. Because if we start to make the use cases a little bit more narrow, so for instance, a specific ability to ask if a named individual looked at my chart. That's going to be really easy for us to do, or even just to look at the sort of where did my data go and who looked at it, that's a lot easier. It gets harder when you start talking about and then, what's the intent of person who looked at it? Because either you're reading their mind or you're asking them to record it somewhere, which gets more challenging from where I sit. So, I think a process around understanding what are the things we really don't want to have happen in the world and a process by which we can all produce information about those specific things that would be very productive, from my perspective.

David McCallie, Jr., MD – Vice President, Medical Informatics – Cerner Corporation

Is there another response, I'm sorry? This is David, just an elaboration on the question. I was thinking about it in the Notice of Privacy Practices that a patient receives at a typical institution lists the broad categories of where data might go. Is there an organizing principle around the Notice of Privacy Practices that would make sense, for example, activity that falls under the categories that are listed in the Notice of Privacy Practices, which typically does not include things like instrument to instrument interfaces, because that's not really considered a privacy issue.

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

David, this is John. I think you're kind of asking the question, if I can interpret and you can verify, are there categories of purpose of use quite literally implied by the Notice of Privacy Practices, both within TPO and also beyond to get at more the traditional accounting of disclosure requirements like public health disclosures, legal subpoenas, things of that nature? So yeah, I think that could serve as an organizing principle. It would take a degree of looking at how any given system knows event types or knows the end-user actions or however you want to characterize them, into those. And very likely, I think some of the discussion about knowing at least what you can to tell the difference between the physician acting in a peer review capacity, which might be healthcare operation versus that same physician acting in a direct treatment manner, where they may be creating or modifying or authenticating clinical data, those are things that probably could be built into it. But as I think others have stated, that is a presumption of either post-processing or pre-configuration of the log information be optimized to make some sense of it. And I do love the idea that make it more about a patient education activity to help them understand what may be useful and then take their requests from there. They may not – I think all the panelists on both first two panels would agree that that's very significant to make utility out of whatever you choose to do.

Paul Egerman – Businessman/Software Entrepreneur

Great. So we have a number of people who have their hands up for questions. So hopefully your questions were responded to David McCallie.

David McCallie, Jr., MD – Vice President, Medical Informatics – Cerner Corporation

Yes.

Paul Egerman – Businessman/Software Entrepreneur

And next we have John Houston. John Houston, are you there?

John Houston, JD – Vice President – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Yeah, I'm here. I appreciate all the great testimony. I guess an open-ended question is, of all the panelists, does anybody really – can they point to customers that have an effective system in place today? And even if not by name, how sophisticated are they, understanding this is a very difficult problem, because I think we do have to be practical and I think that was really what I heard here is that we have to be practical. And so how much can we expect out of this today and what are sort of the best in class people doing?

Kurt Long, MS – Founder and Chief Operating Officer – FairWarning, Inc.

This is Kurt, John. In general, the – and again, my comments are directed more to access reports than disclosure, but in general, HIPAA requires – has a requirement to systemically review the audit trails. In my testimony, I covered many of the uses of internal access reports, so what our best customers do is a very practical approach, knowing that they can't – they – in my opinion the law as currently written, both in terms of the proposed rule as well as elements of HIPAA are not practical. You couldn't possibly comply with them as written because the application vendors are producing audit logs that are so disparate and so different and as I testified, in many cases not at all – and my customers – it's not just a money thing, it's a time and energy thing.

So John, to more directly answer the question is, they identify the applications where the greatest vulnerabilities are, beginning with their electronic health records, that are required to produce that access log. And they produce their user activity monitoring that goes companion with the access reports around the vendors support and where the most sensitive information is, to have a practical internal access report, as well as comply with HIPAA and cooperate with law enforcement. So, identifying the key applications and leveraging meaningful use criteria where you had to have – where they have to produce access logs.

John Houston, JD – Vice President – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Typically how many data elements might you see, if you see a large environment that has 20 or 30 logs that are getting aggregated, how many data elements are we really talking about get imported?

Kurt Long, MS – Founder and Chief Operating Officer – FairWarning, Inc.

It depends, so even for some of the vendors like an EPIC and a Cerner who testified today, they've done such a great job in providing many, many fields in their audit logs, it could be as many as 200. Now in practicality, each and every customer has a little different opinion about which of the fields they would like to use for their access reports and user activity monitoring. Which is usually around 40 fields, but I know that in behalf of our customers, they truly wish for more specificity from the government, and whether that be ONC or OCR, around what is exactly expected of them so they're not just navigating through this with their best efforts. But somewhere around 40 to 50, and some of them will take every single field, which winds up being enormous volumes from vendors like EPIC and Cerner.

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

John, this is John Travis. I made a comment in my testimony that may be, at least from the accounting of disclosures perspective historically. What we've seen in our clients is that probably far more, because of the low volume nature of the request, have a – the better practice, I'll say, has been to have a very well-articulated procedure on where the log data lives, that you would draw on to then go compile the patient-specific accounting. Now that's predicated on two things, one is, that you have time to go develop that patient-specific reporting, so the response time or the service level if you will, is important to that. This isn't a push a button and get it out. And two, I would observe that even with the presence of the logs, if you had a good, well-developed inventory and you had a centralized means of accumulating that data into something you could use for the patient-specific reporting, very high probability you're still going to have orphan systems out there that require some kind of manual data extraction and post-processing.

So I think we need to keep in mind, the point of departure is not the systems we'll be implementing in the next three to five years, but the ones we've got. And those systems go beyond the ones certified for meaningful use, I mean the very nature of what I gave testimony on as a class, are probably not systems by and large being presented for meaningful use certification. They are legacy systems that are in place for ancillary departmental use and even the LIS and RIS systems are probably the better developed of those, that have some decent audit reporting, but the satellite systems used by smaller departments or used as registries are going to be challenged.

Paul Egerman – Businessman/Software Entrepreneur

Terrific. Thank you. You all set John?

John Houston, JD – Vice President – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Yup, thank you.

Paul Egerman – Businessman/Software Entrepreneur

Next we have Wes Rishel. Wes?

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Thanks Paul and thanks to the speakers for focusing on the bread and butter issues that actually make a sandwich here. I've got two questions. One is specific for Kurt and the other is for all four. I'm going to ask them both and then maybe we can start with Kurt and go on. Kurt, you made a comment that the job of consolidating data from multiple systems that produce audit files and producing a meaningful user-friendly output as described in the regulation was a bit of work or some phrases like that. I wonder if you could comment on some measure of the complexity of the implementations you've done, particularly for very large enterprises, multi-hospital corporations. Because the complexity seems to grow geometrically. And when you are done, or when you – typically projects like this declare a good enough a state, when you are done, do you think – what percentage do you think of all the electronic designated record sets you have, that being a much broader category than EHRs called for in the law.

And then the second question relates to chasing the data towards automatic disclosure. So, if you have an EHR and some data is collected, it leaves the EHR, stays within the organization, goes to one or two or three other systems which somehow select some of that data for disclosure, do the audit logs that you're producing now typically audit those kind of batch reports by patient and purpose and things like that? Thank you.

Kurt Long, MS – Founder and Chief Operating Officer – FairWarning, Inc.

Hey John, I'm going to – with regard to the ques – this is Kurt. With regards to the questions that I can offer insight into, I'll start with one of your latter questions first and that is, the percentage – some relative expression of designated record sets. And I'll say at first, for our customers, at the lower end they might have a hundred different applications, maybe in the dozens at the very smallest of applications that touch electronic protected health information and would be included under HIPAA law as well as this – the access report. So when we do a deployment, we might have – it might be feasible to conduct auditing and corresponding access reports for anywhere from 20% to the upper edge, 40% of a given care provider's systems. In other words, the bulk of the systems are either – they just don't produce an access log or it's too expensive or it's too complicated to be worth the time. That's the bad news. On the good news side, that 20-40% of the systems that we're covering probably represent somewhere between two-thirds and 70% of what would be covered under treatment, billing and operations. So that was the first part.

And then with regard to – Wes, with regard to the care providers at great scale, they have a set of unique challenges and those unique challenges include the ones that I've already testified to, but also include the problem of identity – understanding the identity of their users in a unique fashion. And we go hand – our solution goes hand in glove with that category of identity management. So there needs to be, for really large care providers, to be compliant and be able to support to the letter of the law, there would need to be a lot of progress not just in the standards of the access logs, but also into the identity management technologies that are available in the marketplace.

And then closing thoughts, and I'll turn it over is, we're supportive of seeing audit access logs expand. I do agree with Deb when she says there's a set of vendors that would like to participate in this market and bring value. So we would like to see more and more access logs available at very low cost, in a common format, knowing it might invite competition, but that it serves our customers well and it would improve our ability to lower their costs and even provide greater functionality.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Great, thanks. How about the question about chasing the data from EHR to disclosure through multiple systems? Does everybody understand the question?

Kurt Long, MS – Founder and Chief Operating Officer – FairWarning, Inc.

Yeah, I do. With regard to the chasing the data from the EHRs and the disclosure, we're not as expert in that area. Today we have limited visibility of the data that, other than in the context of a healthcare information exchange, which we do support countrywide initiatives in the UK and Europe as well as statewide HIEs in the States, where there is a need – the same kinds of needs for internal access reporting across boundaries. But with regards to disclosures to law-enforcement and to CDC and so forth, we're not as expert at that Wes, we're – .

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

What I'm actually asking is for the question that happens that some part of data is extracted from the EHR for use by other information systems within the healthcare delivery organization. Through the use of those other institutions it ultimately gets disclosed, but the first question is, are those bulk extracts from the EHR recorded in the log? If so, what is the degree to which the purpose is described.

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

Wes, this is John, I'll take a shot at at least one flavor of that, and if it's not on point, please let me know. The reporting of public health data, I spoke of reportable labs, most typically they could be reported in real-time, but most typically they're going to be done periodic, large batch. It is possible that the submission files may be retained, it's possible that some type of almost shadow run, if you will, could be retained and the metadata about the submission as to who the patients were, what kinds of data, when the date occurred. But our experience is those typically get maintained as reflective of that submission event. So the systems that do public health reporting most likely have logging of the public health reporting submission and an ability to retain the submission file, or some kind of almost registry listing kind of thing of the submission file, but they're not in a patient-specific context. To make use of them, to participate in a broader compilation of an accounting and disclosure to the patient would require you to cross files that reflect individual submission events.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

John, I'm actually asking a simpler question.

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

Okay.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Does your audit log record all of the information accesses that happen during batch extraction of data from your system?

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

As machine operations, I don't believe that they do for extraction, absent the retention of that actual extraction file. For the turn around to submit to the public authority, the possibility is there.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

So when the data is disclosed directly from the EHR, you may have that ability, but when it goes through other systems on the way towards some disclosure, we would rely on those other systems actually doing their own –

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

That's a fair point.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

– logging, it wouldn't be part of your log and then every other system that's involved would have to be remediated for this process, even though they're not EHRs.

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

To get the full chain from source system to external submission, considering that there could be one or more contributing systems to it, I think that's a fair statement. So –

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Thank you.

Paul Egerman – Businessman/Software Entrepreneur

And Wes, your question is a good question, because when we think about the security logs, the tendency to realize that gee, these are logs where some person or something is logging in an authenticated access to the system. But there are many kinds of data that's simply transmitted, in which case there is no entry in the security logs or most security logs.

(Indiscernible)

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Paul, I would also point out, Paul I'd also point out that the process – the steps to disclosure could go through several systems, none of which has a person involved, these are all what we used to call demon processes, batch processes.

Paul Egerman – Businessman/Software Entrepreneur

Yes. I understand, very helpful question and comment. In the queue right now I have Leslie Francis, Deven McGraw and Walter Suarez and also Linda Kloss. First we'll do Leslie. Let me ask everyone to just ask one question so we can try to get as many people involved.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

This is Peter Kaufman, I've had my hand raised for quite a while and it's not –

Paul Egerman – Businessman/Software Entrepreneur

Okay. Somehow I don't see you on the computer, but I will make sure we get to you Peter. Thank you.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

My question was to some extent anticipated by the last discussion, but I'd like to hear everybody comment on. To what extent it does seem reasonable, feasible to go with the kind of suggestion that Deborah Peel was making, that really the burden is not all on the vendors, if there were access logs available, consumers might well develop – or consumer-oriented software providers might well develop a suite of tools to help people make sense of it.

Stephanie Zaremba, JD – Senior Manager of Government and Regulatory Affairs – athenahealth, Inc.

This is Stephanie Zaremba from athenahealth. Jeremy had to step out, so I apologize that you're now stuck with me. But, I'll take the first shot at that question. I think the biggest challenge from a technical perspective with what Dr. Peel proposes is the sheer volume of data and where it's going to be stored and at whose expense it's going to be stored. So these audit logs do exist. Integrating them into sort of an on-demand system like she's talking about, I completely agree that there could be a number of companies that would develop a tools around that to make it more user-friendly, to make it more accessible. But if I understand her proposal correctly, it's to have not just the audit log, the access trail, but a copy of the information that was accessed, user-disclosed and that, I mean you heard some of the numbers thrown out by the various testimonies just now. Quickly thousands upon thousands of not just accesses, but then the

information that would have to be stored with them, that would be a real challenge.

Kurt Long, MS – Founder and Chief Operating Officer – FairWarning, Inc.

And this is Kurt from FairWarning. In response to that specific question, when it relates to the centralization access of our customers access logs, because we're a privacy and security company, and that information is related to privacy and security, that's certainly information that we've always treated with the utmost of confidence and would never want to publish. That seems like a contradiction to a privacy company that publishes the access logs of our customers somehow that doesn't make sense. But, what might lend itself to a more robust community of developers in this area is ubiquitous data standard that's well-known and well understood that's publicized and other software developers could develop against. That doesn't compromise the privacy and security of care providers, right, so just so that there's a common API or a common standard and format that they can count on being there is something that we think is more powerful .

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

This is John Travis at Cerner. I think just to offer again, to make it usable, the toolset would have to address the normalization, I think that's some of what's suggested as potentially the standardization of that format or those data columns. But to make sense of the – username either being a person or a machine process or a system and normalizing purpose of use and normalizing all the event types that each individual system is not going to have the same point of reference to say what a modify is or a signing event. There probably could be pretty common standardization, but certainly any tool to be useful is going to need the ability to normalize the references of the data columns to make it consumer-friendly, if any of those tools were to be put into a consumer's hands.

Paul Egerman – Businessman/Software Entrepreneur

Terrific. Thank you very much. Thank you for that question Leslie. Next we have Deven McGraw.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Yes, thank you. I'm glad to be back online, so for those of you who are still hanging – are not able to get in, keep trying, attrition is happening and you're able to get on. I have a question related to whether there's a stepwise approach that we can take to this from a technical standpoint. So let's say we assume that we might rely on audit trail technology, such as what is already required to be in certified systems to be the baseline for a set of policy recommendations around transparency. Is there anywhere where we can go from there in terms of improving the way that that log functions or its capacity to serve sort of multiple roles, both in terms of allowing entities to do their internal security work but also serving some transparency needs of the patients as well?

Kurt Long, MS – Founder and Chief Operating Officer – FairWarning, Inc.

Hey Deven, this is Kurt. I'm trying to give everybody a chance to respond but this happens to be a topic that we've thought about an awful lot. And we think that the only way toward a practical access report as proposed in the rule, and we already testified we don't think it's feasible today. We think – so, over time, this has to be something that's considered over a two, three, four, five, maybe even a 10-year time horizon to build the support for the data required in the access logs. And to allow the vendor community to catch up and build it into their product plans, which in our opinion they sh – we all should be producing access logs as long as we're serving US Healthcare, including FairWarning. And we need to take a longer time horizon that bring in phased functionality, beginning with the very simple functionality of what's technically feasible today and then looking out over time to say in some of these more detailed, nuanced cases, perhaps we can get there. But if the data's not there for our customers, I know that we and they just can't do it.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Thank you. Appreciate it.

Paul Egerman – Businessman/Software Entrepreneur

Great. And in the queue right now I have Walter Suarez, Peter Kaufman and Linda Kloss. And so we'll do Walter next.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Paul, can you please add Lisa Gallagher to the queue?

Paul Egerman – Businessman/Software Entrepreneur

Lisa Gallagher, yes. Walter.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

Great, thank you – yes, can you hear me Paul?

Paul Egerman – Businessman/Software Entrepreneur

Yes.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

Yeah, thank you so much and thanks for this really excellent testimony. So under the current HIPAA regulations we must account for, all covered entities, for certain disclosures. And then under the HITECH provision, those were extended to now include or intended to include treatment, payment and operations disclosures. And then we have this proposed regulation that extended even farther that from disclosures to these additional thing called the access report. And you all highlighted in very good detail some of the significant challenges and issues associated with trying to document and report every instance of a use of health information and then report back to the consumer.

What I wanted to ask is about the disclosure part, because I think the disclosure part goes through a little bit of a different, in many cases, quite significant different processes and workflows, from the audit log that captures who has accessed the records. Because disclosures in many cases happen by virtue of preparing a report and then sending it out, whether it's to a payer or to another provider or to public health or to some other entity outside. And it's different from the so-called access, which is a word that we have used quite bit in this hearing. So could you comment on how would your systems attempt to capture and maintain documentation about the disclosures for this expanded TPO? And to what extent there will still be some manual processing needed in order to list and to identify and document those disclosures than for TPO.

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

Walter, this is John Travis. I guess maybe I'll take that one first. I think that two observations; one is, and I'm very curious to know if OCR will reconcile this. We're really going to wind up seeing two accounting of disclosures requirements, and I'd argue in a lot of ways the one being proposed now is covered by the first one. Or at least there's nothing that could have prevented a patient from asking for electronically based disclosure activity to be included in the original HIPAA privacy right to the accounting. But I think there is information that is different between the two logging purposes that may not always be available in the security audit log that gets more at a direct purpose of disclosure, potentially, depending on the nature of it.

So doing a disclosure for a legal subpoena, doing a disclosure for public health, I think that it's much tighter to purpose to know that when I'm doing public reporting of lab results out of a public reporting function or to a registry or for quality measures. I can pretty well know what that disclosure pertained to, even though the information might be implied, based on the metadata I have, I know what I am doing there. But I don't know that that kind of information is real available always in a security log that's really tuned to be designed to support internal security, policy review for compliance purposes under the Security Rule. So one – and then I think your disclosure log sources are going to be much more diverse because certainly that reporting can occur from all over the organization. It – chances are it may historically be something that's being only partially maintained electronically. It may also be maintained manually.

And so I think organizations are going to look for a solution to the problem of the accounting of disclosures as best they can, still driven by a procedural answer to it that they've seen historically versus some kind of large central logging, given the low volume historically of that request. And what I found interesting with the OCRs proposing it applied to the designated record set and not what may be seen as the EHR, certainly not confined to what is EHR under meaningful use.

Stephanie Zaremba, JD – Senior Manager of Government and Regulatory Affairs – athenahealth, Inc.

This is Stephanie from athenahealth, if I can just add to topic. Walter, speaking from less the system, my perspective and just getting at what our EHR can do. Our EHR and privacy management system that producing an accounting of disclosures, even for treatment healthcare – driven payment healthcare operations is much, much easier than providing a full disclosure of all access, that full audit trail. That's a functionality that exists today. The optional meaningful use EHR certification criteria that was mentioned, we have that, so I think as we're looking at options of what's possible, looking at disclosures from one system is actually a lot easier and much more automated a far less manual process that our providers can do, kind of on demand with their patients right there .

Eric Cooper – Group Lead, Software Development – EPIC Systems, Inc.

And this is Eric from EPIC and I wanted to make a point. I think when we discussed disclosures versus access, one of the key distinctions, and some of the proposed legislation around it, stating whether or not the user is employed or not employed by that organization, comes into play. And that's why you necessarily can't distinguish between the two, you have to talk about both. Trying to distinguish that a use by a non-employed user that's on the same system would then become a disclosure, inherently makes it a problem that we're looking at the breadth of what the access log functionality can cover. And I think that's where we start to focus our attention more on the access log side of this than on disclosures. Because I would agree that a traditional disclosure is something that we all can track well and can do, although we do have a system to track that and is well defined, when you're sending a person's record outside of the system. But when you start getting into the – talking about employed, non-employed, I think it becomes very difficult.

Paul Eggerman – Businessman/Software Entrepreneur

Yeah, although it's not necessary – this is Paul, it's not necessarily the case that a non-employed person is a disclosure. There is this concept of the OHCA, the organized healthcare arrangement, and they might be within the OHCA, but that's a whole other story. The real issue is, what is the boundary that causes a disclosure, if there's ambiguity about that and confusion about that.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

Yeah, well thank you so much. Thanks to everyone.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Paul –

Paul Eggerman – Businessman/Software Entrepreneur

Excellent comment. Now I still have Peter Kaufman .

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Paul – .

Paul Eggerman – Businessman/Software Entrepreneur

Just a second –

(Indiscernible)

Paul Eggerman – Businessman/Software Entrepreneur

Just a second Wes. Peter Kaufman, Linda Kloss, Lisa Gallagher in the queue. Deven, how much time do I have left here, I'm a little confused on the schedule. I have two copies of the schedule, I go to 2:30 to 2:40.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Hold on, I will tell you – you go – the provider panel starts at 2:40, you can take a whole –

Paul Eggerman – Businessman/Software Entrepreneur

At 2:40, okay. So I know you're trying to say something Wes, did you have something very brief?

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Yeah, just Joy made a point of correcting me this morning and I appreciated it, that a non-employed physician using the EHR is a disclosure that came as a surprise to me.

Paul Eggerman – Businessman/Software Entrepreneur

I'm not sure. That's a –

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Yeah, no, it can be, that's one of the policy issues that we can discuss.

Paul Eggerman – Businessman/Software Entrepreneur

Yeah, I mean, I'm not sure. If a radiologist –

Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Health & Human Services

Paul, excuse me this is Joy and Linda Sanches, who is the OCR – who is here agreed with me, so, let's just move on for the time being.

Paul Egerman – Businessman/Software Entrepreneur

Okay, let's go on to Peter Kaufman.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Hi. Thanks very much. I'm going to change the track just a little bit, and I didn't hear anything about this but part of the standard is for business associates to be transferring the disclosure and access information to the EMR for the EMR to provide to the end-users. And I'm not aware of any standard for this to happen. The standards take a while to generate and if this isn't done in a standards-based way, there's going to be no way to get that data into the EMR in a way that's usable. So I just also wanted a voice for some discretion in adding that at any time in the near future, but encourage people to work on a standard for this kind of data, so that it could be transferred electronically between systems. There may also be a time when there would be – if patient's wanted to have access to really full accounting of this, that the EMR through a standards-based system might be able to transfer it securely to a patient-based system that the patient would purchase. And then be able to have further access than they would, as described by EPIC, which would be a more focused search for disclosure and access. I'm done.

Paul Egerman – Businessman/Software Entrepreneur

Okay. Thank you Peter, very helpful. Linda Kloss? Are you there Linda?

Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.

Yes. Thank you. Excellent discussion. And my question really related to what Peter's comment just was, that one of the most advanced processes for external release of information is often outsourced by organizations to business associates. Who then, you would presume, we would want to track the purpose and the categorization of those particular release of information, disclosures, back into that EHR and just wondering if anyone is doing that now and whether they're adopting any standard categorization or processes for doing that. And my second question really related to our first panel, where there was quite a lot of emphasis on particular information on disclosures through health information exchanges and if we could comment on that dimension. Thank you.

Paul Egerman – Businessman/Software Entrepreneur

Do we have any response to Linda's comments?

Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.

The first is the release of information function where the information comes from the EHR to the business associate, is the getting logged back in detail?

Eric Cooper – Group Lead, Software Development – EPIC Systems, Inc.

And this is Eric from EPIC. We do track disclosures to the health information exchanges today, but we also have, when they're doing the external release of information maybe outsourced, they typically record the disclosure in their system, but also in our system as well. And that's usually done through a manual process, there's some synergies around that, but it's typically done both manually in two different systems today.

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

This is John Travis. At Cerner I would echo that –

Stephanie Zaremba, JD – Senior Manager of Government and Regulatory Affairs – athenahealth, Inc.

We'll change that to –

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

– sorry?

Paul Egerman – Businessman/Software Entrepreneur

Why don't you go ahead John, I think Stephanie was also speaking, but first –

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

Oh, okay. No, I'm presuming that you were speaking of the kind of release of information vendor that a lot of healthcare organizations will engage with to manage formal –

Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.

That's right.

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

– releases. Yeah, I think that we've seen two things true. We do have the ability to record that release within our system through tools that are used, whether the HIM functions being performed within or outside the organization. Certainly we're also seeing that those external business associates also typically have that ability to record and log and they're obligated to make that information available for consolidation into the accounting of disclosures given to the patient. So, we've seen it done both ways.

Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.

So, you think that part of the process is now working?

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

That process is actually very specific to the traditional definition of the accounting of disclosures where those functions are used, so if you – and I even think that the OCR reflected very well what kinds of disclosures those are in their proposed rule for the accounting of disclosures part of the NPRM. I think that part of it, when it comes to use of a structured formal business associate for release of information, we've seen works fairly well. And I think it's an even mix of whether or not they record it back or their using – whatever system or software they're using to manage those requests externally, those systems do typically have that ability, from what we've seen. So the reporting could come from either place, the EHR or the systems and tools being used by the business associate, because often times they are using a distinct system to record those events.

Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.

And the information for the patient would be similar?

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

Yes.

Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.

Would be aligned, and that may be a model –

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

Yes, I believe – part of it is they're much more attuned to the formal – the thing you'd think of naturally as what a disclosure is, is the information being physically disclosed. Now within that is the additional logging of the disclosure event from the EHR to the business associate, which would fit more on the access report in the traditional definition, or in the framework of the NPRM, I should say.

Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.

And the HIE, you indicated you were doing that now?

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

That was EPIC's response, but I think we would respond similarly.

Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.

Thank you.

Paul Eggerman – Businessman/Software Entrepreneur

It's okay, you all set Linda?

Linda Kloss, RHIA, CAE, FAHIMA – President at Kloss Strategic Advisors, Ltd.

Um hmm.

Paul Eggerman – Businessman/Software Entrepreneur

Great, and next we have Lisa, was it Gallagher?

Lisa Gallagher, BSEE, CISM, CPHIMS - Senior Director of Privacy and Security – Healthcare Information & Management Systems Society

Yes. This is Lisa Gallagher from HIMSS, I'm a member of the Standards Committee and the Privacy and Security Workgroup of the Standards Committee. First I want to say this has been a very compelling panel and I appreciate everyone's dialogue. In hearing what I've heard, I almost didn't ask this question, it probably would have been best for the first panel, but given Deven's questioning about what can we phase in over time. So we heard a lot today about the fact that with regards to the access reports, there are a lot of technical challenges. And also it occurs to me there may not be especially good alignment between the requirements for the access report and the requirements of the meaningful use EHR certification, at least as it stands now.

But I would note that meaningful use – future meaningful use stages do require a list of the care team members and the ability to view, online and download and transmit patient data. So with regard to the actual patient's privacy interest that we're going after here, what are the panelists thoughts on – is this a significant enough advance and transparency to really – to answer a lot of the questions that are there for access? And given that we've said – many have said we can implement the accounting of disclosures a little more easily, is that something that, given its down the roadmap, workable alongside of accounting disclosures to meet the true privacy interest here?

Kurt Long, MS – Founder and Chief Operating Officer – FairWarning, Inc.

This is Kurt from FairWarning and I'm not going to weigh in. We've already testified on our – what we think the value of access reports is to information security, privacy and compliance. And we've already said that, and probably not technically feasible – technically feasible for the proposed rule. Having said that, the conversation and all the underlying work that we're doing has tremendous value to privacy and security, even if the evidence of it at first is just a very – if any, external access report requirements. So in other words, these are – the conversation we're having, we have to have as an industry to secure privacy and information security and quite frankly, comply with HIPAA. It's just that so much more work needs to be done before you could ever get to the dre – I'll call the proposed final rule kind of a dream state thing. So I think you've got to do both, Lisa. I think you have to keep doing the heavy lifting technically and deliver incremental functionality about what's feasible and affordable to care providers, but you've got to take a longer term view. So yes, I think it's all worthwhile.

John Travis, FHFMA, CPA - Senior Director and Solution Strategist, Regulatory Compliance – Cerner Corporation

This is John Travis. I'd offer the comment, as an incrementalist strategy definitely focusing on the things that go towards end-user or natural person as I think I characterized it access events, as a starting point, not an ending point. And building from there and really use that as the opportunity to develop the guidance around how best to normalize usernames, IDs, roles, event names and types, data types, the things that are important data columns on the report. And even to do I think an outreach, I think this would be a patient right that could be tremendously useful in a targeted – to target answers to the patient's questions of who's seen my record of a particular, specific interest and avoid it being the data dump exercise. But then it also could be, for that reason, a tremendously confusing right to exercise without a lot of support and assistance from the provider, from potentially the Office of Civil Rights and patient advocacy groups. So it's not something very many patients are going to be equipped to just say, give me my report and make sense of, so I think – starts on the things that make more sense perhaps, or arguably and the things that can go towards recommended practice guidance both for patient education and normalizing the data for patient consumption.

Stephanie Zaremba, JD – Senior Manager of Government and Regulatory Affairs – athenahealth, Inc.

This is Stephanie from athenahealth. And I want to apologize briefly to Linda, at your previous question, I was disconnected for a moment, so I apologize for not getting a response in to that one. But Lisa, as we look at an incremental approach, I would just add on, I think it's very important that we always come back to the question of, what is going to mitigate against the risk of improper access and what is going to be meaningful to patients? So absolutely agree that focusing on human to human interaction where PHI is being disclosed is kind of the obvious first step. But, it – just because we have everything in electronic access doesn't mean it necessarily benefits the patient to just dump it on them. We really need to be thinking about this through the lens of having it be meaningful and having it be useful for mitigating against the harm we're trying to prevent.

Paul Egerman – Businessman/Software Entrepreneur

Terrific. Are you all set Lisa?

Lisa Gallagher, BSEE, CISM, CPHIMS - Senior Director of Privacy and Security – Healthcare Information & Management Systems Society

I'm all set. Thank you.

Paul Egerman – Businessman/Software Entrepreneur

Great, and is there anybody who wanted to ask a question that I somehow didn't call on? Nope, not hearing any response, I hope everyone got their questions answered and I just want to thank the four panelists again. This has been a very compelling and important discussion. You provided a great deal of information, which is very much appreciated. So Deven, are we on to the provider panel? Are you doing that?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

I think we are. So, I can do the – I got kicked off the line again, just like Stephanie just did. So I'm certainly happy to announce folks, it'll just be a little bit harder for me to manage the queue. So I'm wondering if you can pinch hit on that aspect of it?

Paul Egerman – Businessman/Software Entrepreneur

The queue, yeah, no problem.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Okay, that would be extremely helpful.

Paul Egerman – Businessman/Software Entrepreneur

As long as you continue to do the rooster part, because I cannot do that part.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

I can do the rooster. I'm happy –

Paul Egerman – Businessman/Software Entrepreneur

And you do it so well.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Well thank you, I appreciate that, it's such a difficult task. I will continue to time folks, but I'll go ahead and do the role of announcing the panel, because I'm at least equipped with my own hard drive to be able to do that, so thank you. All right. Well we have first up in our provider panel, and this is a slightly bigger panel by one than the previous panel, but we have allocated a little bit more time. Unfortunately, people are still limited to five minutes, and as Paul mentioned, you'll hear the crow of a rooster when you have 30 seconds left, and we'll appreciate you wrapping up within that time and we'll pick up any points that you're not able to make in your testimony in the Q&A portion. So we're starting with Darren Lacey, who's the Chief Information Security Officer of the Johns Hopkins University Health System. Darren, are you on?

Darren Lacey, JD – Chief Information Security Officer – Johns Hopkins University Health System

Hello, can you hear me?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Yeah, we can hear you just fine.

Darren Lacey, JD – Chief Information Security Officer – Johns Hopkins University Health System

Marvelous. Thank you. Thank you for the opportunity to speak. It's been educational, I've learned a great deal in this already. My principal reason for getting into it is that if I was going to be responsible for helping put together a strategy for addressing this, that I ought to at least know what you're looking at doing. I think I had some contribution to make, I'm just the security guy here, so I'm not – I'm probably not as up to speed on some of the policy issues, but I'll – basically I think I'm here to at least amplify some of the things that were said in the last panel, but I'm going to have some remarks here. I pretty much look at logs all day it's what I do. Hopkins generates about 2 billion security events, billion with a "B" a billion security events per day for things like network security logs, server attacks and other typical types of security events. Now fortunately, most of those aren't access logs, which numbers in the several hundreds of thousands to about a million a day. So, it's still a significant number, it's still a big data challenge.

And the reason I bring this up, I understand the distinctions that we have to make between disclosures and the user access reports. But in both cases, and I think they are quite a bit different in terms of maybe which are easier to do, but in both cases, they are actually operationalizing logs, making them sort of public in some sense, trying to sort of work through them. But logs are – but to me that reflects some – a problem with actually logs are viewed by people who do security for a living, which is we don't – we view logs as essentially being probabilistic and probative and not determinative. We don't actually look at logs as the end-point, well, now we have a log and that proves that this happened. We actually look at logs a lot differently than that. We say, okay, well this log says this and we're not sure exactly if that's the whole story, we don't know if that person logged in in that way or if they were on that machine, let's see if we can find some other logs that will help indicate that.

We use this approach because we – to essentially serve two purposes in the security field and privacy practice to some extent, we focus – we conduct focused investigations based on exigencies, based on complaints, tips, things that come up. A lot of times we'll just do an investigation because they'll be a particular user that's famous, I think most of you are aware of those types of investigations, but we conduct investigations routinely, it's part – we have staff who do that, most large medical centers have staff that do that. It's a little more difficult for smaller provider organizations to do it, but they also conduct investigations. And we also use it to detect use anomalies, and this is an area where I think folks like FairWarning and frankly the other pa – have had a big impact. And also the consolidation of some IT around meaningful use has also had an impact, because we've been able to pull together maybe a smaller number of designated record sets, a smaller number of records, to be able to start to really look and see, wow, can we, without prior knowledge, see uses that may be problematic. And in our environment, that's what I do, I spend a lot of time working on that. I work on a research product with some leading research institutions called the SHARPS Project, on just this subject. And we employ machine learning, we employ advanced statistical analysis to try to detect these anomalies.

And so our feeling is that logs actually provide a useful – are the core for that, and they're the core for all kinds of metadata analysis like you see in Silicon Valley for people essentially determining the efficacy of how certain applications run and how systems work. And we follow that approach fairly closely. But what we don't do is, we don't come in and say, oh, these logs – oh, okay, great – these logs actually tell us everything that we need to know. Or they tell us everything that if you didn't have professional people around actually looking at them and trying to – and using tools to help them make sense of them in the context of the specific provider. And say, this is how – this is the determining state and this is where – this actually accurately reflects what happened in this particular case. All right, I'm done.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Thank you very much, we appreciate it Darren and glad you can stay for the Q&A because I suspect there will be some questions for you that will allow you to elaborate on the points you just made. Okay, next up we have Lynne Thomas Gordon, who's the Chief Executive Officer of the American Health Information Management Association. Lynne, are you ready?

Lynne Thomas Gordon, MBA, RHIA, CAE, FACHE, FAHIMA – Chief Executive Officer – American Health Information Management Association

I am, good afternoon.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Good afternoon, can you move a little bit closer to whatever microphone you're using.

Lynne Thomas Gordon, MBA, RHIA, CAE, FACHE, FAHIMA – Chief Executive Officer – American Health Information Management Association

Okay, how's this, is that better?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Much better. Thank you.

Lynne Thomas Gordon, MBA, RHIA, CAE, FACHE, FAHIMA – Chief Executive Officer – American Health Information Management Association

Oh great. Okay. Well thank you for so much for the invitation to testify today. We at AHIMA applaud you're convening this hearing to discuss the important issues of disclosures. Just a little bit about AHIMA, we're 85 years old and we're a not for profit association of more than 67,000 professionals who are educated, trained, certified and working in the field of health information management. And our members are employed in multiple settings across the healthcare industry. We are recognized as an unbiased, trusted, authoritative source, not motherhood and apple pie, but about as close to it as you can get. Our members serve on the front lines and they oversee privacy and security requirements and adherence to federal and state laws. AHIMA is committed to several foundational principle and tenants, and especially data integrity and data confidentiality and these principles are the basis of our comments today. So I'm going to focus my remarks on two primary areas, one is just the balance of disclosure versus burden and the other is workforce safety.

So to begin with, our first comment really does regard the balance of disclosure versus the burden. AHIMA and its members are advocates for privacy, security and confidentiality of health information, and we have been for our entire 85 years. Regarding accounting of disclosures, AHIMA believes that individuals really do have a right to ask questions and seek an investigation regarding who has accessed their protected health information, or PHI. We support the investigation of any reported inappropriate use or disclosure of PHI as currently required by HIPPA. However, we believe that the investigation undertaken must consider several factors. So we think it should include the nature of the alleged disclosure, the potential burden of conducting the investigation and providing a response. And believe it or not, the safety of the healthcare workforce.

So the accounting of disclosures proposed rule included the right to an access report. AHIMA believes that any requirement for access reports exceeds the HITECH statutory language and would likely be expensive to develop, implement and maintain. We are concerned that compliance would require covered entities and business associates to make major and significant information technology and systems modifications, as well as workflow and process changes that will significantly increase administrative burdens and cost. We are concerned that such a burden would be incurred for what would likely be a very small number of requests, and I think we've heard that today, that the requests are really not as much as we anticipated. Further, we believe that capturing and providing granular and detailed information on every internal exchange of data would be challenging.

We feel it is much more feasible to respond to access requests on an as needed basis and in instances where there is a reasonable indication that inappropriate access has occurred. We are concerned that routinely providing an accounting of disclosures of access reports for all patient requests for all transactions does not meet the burden test established in the statute. We strongly suggest that any accounting of disclosures and/or an access report be provided in person to the requesting individual, so that it can be fully explained. AHIMAs members who are compiling access reports tell us that they are unwieldy, they're very long and they are burdensome to create. Furthermore AHIMA believes that there is a need to educate patients about the definitional differences between the use and the disclosure of personal health information. And of course, many of our speakers today have talked about that as well.

These terms are often used anonymously and that can create confusion.

I'd also like to focus on a second area and that is ensuring the safety of the health care workforce. AHIMA believes that identifying specific workforce members in an access report could unnecessarily jeopardize the safety of those persons. If the final rule were to require the identification of all individuals, AHIMA believes that any – report should not include individual names. AHIMA members tell us that when patients seek disclosure reporting, they often have a specific individual in mind, for example, their neighbor or a family member, etcetera. We believe that with the current breach notification requirements, organizations should already have policies and procedures in place for investigating any reported potential breach. Based on the breach investigation outcome, current breach notification requirements require complete follow through of all reported incidents.

So in conclusion, we appreciate you providing – letting AHIMA comment today and testify. And to augment our testimony, we have supplied the team with several additional AHIMA resources related to these questions. And we stand ready to work with you on this critically important topic. Thank you.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Thank you very much Lynne, much appreciated. Okay, next is Jutta Williams, who is the Director and Corporate Compliance Privacy – she's the Director, I'm sorry, of the Corporate Compliance Privacy Office and the Chief Privacy Officer of Intermountain Healthcare. Are you on and ready?

Jutta Williams, CISSP, CISA, CIPP – Director, Corporate Compliance Privacy Office and Chief Privacy Officer – Intermountain Healthcare

I am, can you hear me all right?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Yeah, we can now. Thank you.

Jutta Williams, CISSP, CISA, CIPP – Director, Corporate Compliance Privacy Office and Chief Privacy Officer – Intermountain Healthcare

Wonderful. Thank you so much. So my name is Jutta Williams and I am that Chief Privacy Officer at Intermountain Healthcare, which is a not for profit, community based, integrated healthcare delivery system headquartered in Salt Lake City. We 22 hospitals and more than 185 clinics and we employ approximately 34,000 healthcare professionals who provide care to more than 6 million patients each year. Perhaps because we began to adopt an electronic medical record more than 30 years ago, Intermountain has long understood and respected it's data stewardship responsibilities for safeguarding electronic protected health information. We continually refine and improve our policies, procedures and adopt technology and have invested quite substantially in a comprehensive HIPAA privacy and compliance organization.

We currently employ about eight full-time people and up to 20 part-time privacy team members whose responsibility is specifically to focus on interpretation and enforcement on HIPPA Privacy rules, to identify inappropriate behavior and investigate concerns or complaints. For more than a decade, we've maintained a robust, proactive – appropriate access identification response program. I talk to patients about their privacy concerns pretty much every day. My personal experience talking with patients and overseeing resolution of literally hundreds of concerns and questions over the last several years is that patients have not expressed a general sense of curiosity about how their information is used appropriately or even how it's disclosed for routine treatment, payment or healthcare operations related purposes.

Over the past 10 years, we have received 11 requests for an accounting of disclosures under current law, or about one per year. What patients have demonstrated an interest is the investigation of a specific privacy concern. About a hundred times a year, patients express to me that something specific occurred in their lives that concerned them. They generally know who, when and where an inappropriate access may have occurred and are interested in understanding whether information about them was used or accessed inappropriately. They want to know that their concern was heard and was then thoroughly investigated and that appropriate action was taken by us when an employee acted improperly. They're relieved when I can share with them that nothing inappropriate did occur. Importantly, we do not specifically name employees when we report information back to patients, nor do we include individual employee names in breach notification letters today, which is not required under HITECH Breach Notification Rule. This is right and correct since we the company must be positioned to take ownership of an employee's actions, especially for someone who has acted inappropriately and in violation of the trust we placed in them, and that the patients have placed in us.

I applaud AHIMAs comments about employee's safety and I want to emphasize the same point. Intermountain has made a risk-based decision to not even include last names on our badges in order to limit our employee's exposure to potential harm or harassment by patients. By requiring access reports to include the name of employees, a proposed right to an access report exposes our named employees to risks, particularly in rural areas, of being tracked down and potentially harmed. Because of the lack of contextual information in an access report that explains why a healthcare employee may have accessed a record, a patient may feel justified in contacting healthcare employees directly to ask why they saw the patient's PHI.

If a patient raises a privacy concern based on an AOD or access report, then the covered entity should be responsible for investigating that concern and for the patient – excuse me – on behalf of the patient and reporting back to them. This gives us the opportunity to address patient concerns, make any needed adjustments in our privacy processes and take appropriate disciplinary action. This is recourse that's not available to a patient if they were to conduct investigations on their own. Regardless of what else may come from this hearing, I beseech the committee members to exclude names of employees from any alternative you consider.

I'd like to shift my testimony now from patient privacy interests to provider burden. The belief that all systems are capable of providing inquiry or read level audit data is flawed. The Security Rule does not require this capacity and struggled with players to require it as part of a purchase decision, rather the rule requires that we "conduct a system activity review." The Security Rule is flexible, scalable and technology neutral and does not require read-level audit capacity, nor does the Meaningful Use Program. Thanks.

To upgrade systems such that we can deliver record level inquiry audit data for health information technology systems as proposed, and to purchase the consulting services needed to develop and implement an expanded enterprise log correlation capability is costly. We estimate Intermountain's cost to be, at a minimum, of \$100 million dollars or five times the OCR's estimate for the entire nation to implement the access report provisions of the NPRM. To put that cost into context, that's three times the cost of ICD-10 conversion, fully half a charitable care budget for a year and the cost of building an entire rural hospital. It's Intermountain's position that currently available technology –

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Jutta, I need for you to just wrap up, you'll have lots of chances to make more points during the Q&A.

Jutta Williams, CISSP, CISA, CIPP – Director, Corporate Compliance Privacy Office and Chief Privacy Officer – Intermountain Healthcare

Understood.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Thank you.

Jutta Williams, CISSP, CISA, CIPP – Director, Corporate Compliance Privacy Office and Chief Privacy Officer – Intermountain Healthcare

Please just understand that context is not available and the question of why is not appropriately addressed by technology, only by interjecting human interaction with a person we can deliver the answer of who, but not necessarily why. And I'd be happy to answer more.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Great. Thank you very much. Next we have William Henderson who's the administrator of the Neurology Group in Albany New York and also the Co-Chair of the Board of Directors of the Medical Group Management Association. William, are you on?

William Henderson, FACMPE – Administrator - The Neurology Group, LLP (Albany, NY); Co-Chair, Board of Directors - Medical Group Management Association

I am.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Oh terrific, and we can hear you just fine. You ready?

William Henderson, FACMPE – Administrator – The Neurology Group, LLP (Albany, NY); Co-Chair, Board of Directors – Medical Group Management Association

I am.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Go ahead.

William Henderson, FACMPE – Administrator – The Neurology Group, LLP (Albany, NY); Co-Chair, Board of Directors – Medical Group Management Association

Thank you for allowing me to speak to this esteemed group today. I am the Administrator of an eight physician, single specialty neurology group in Albany, New York. We have about 25,000 patient visits per year in our offices and we've been using an integrative practice management and electronic health record, and some of my providers have done so since 2005. In addition as was mentioned, I am Co-Chair of the Medical Group Management Association Board. In that capacity I am in contact with hundreds of practice and group leaders regularly. One of the matters I will comment on today, MGMA did a research questionnaire of its members on the very issues being discussed. The I will cite in my testimony come from representatives of 1400 groups representing 30,000 physicians. MGMA also submitted the results of this questionnaire to the Office of Civil Rights during the formal comment period on the Accounting of Disclosures Proposed Rule. For the convenience of the panelists and public today, I've submitted the August 1, 2013 letter to delineate our position

We can look at the questions that have been raised by the Tiger Team under three general categories, what's the current environment for our patients, what do they need or ask for? What is our current capacity – capability and tracking the use of patient's health information? And what would it cost us from a financial and resource perspective to provide what this regulation appears to demand? Well first, a critical point, as a provider of healthcare, we are patient-centered and take the federal regulations that are issued quite seriously. Part of our responsibility is to inform our patients about their rights. In 2003, when the first HIPAA requirements came out, we hired a 0.5 FTR staff member whose sole job it is to speak with the patients about their medical record questions and to document the release of all non-PPO medical information, so we could provide an accounting to those patients who requested such disclosure.

In the first 10 years that we've had that project, we've not had one single request for such an accounting. In fact, in the last decade, we've only had one individual even request a restriction on who could have access to their medical record, and that was a request we accepted and processed. Our experience correlates with 65% of MGMA associated groups who reported one or less accounting reports requested in a 12-month period. Our group's Notice of Privacy Practices informs patients of their access rights to their health information.

Second, we also protect patient's health information by disclosures by limiting the scope of patient's records that a staff member can access, to the extent that we currently have the capability to do so. For example, clinical staff can view all the patient's record because they may need billing information, but a receptionist does not need to know clinical information. Currently we have no built-in computer based capability to track the use of patient's health information, especially for TPO. Our designated staff member is tasked with documenting non-TPO disclosures and tracks all these releases manually. Now it is true that most of our patient's information is recorded and maintained electronically. We use an integrated system.

On the clinical side, we can run what are known as activity audit logs and these reports are geared to identify what particular users did and thus report this way. For example, we can run the report on the activity of a particular employee, but we don't have an audit tool that can show the activity by a particular patient to view disclosures. We don't have the ability to create and save a report of who accessed a patient's record in our EHR or a description of the action they took, or why they were in the record. Moreover, we cannot currently track every person who has viewed or taken action when a patient's insurance or guarantor billing, information that would be part of the HIPAA defined designated record set. This real limitation is consistent with the capabilities reported by participants in MGMA's questionnaire. One item of concern is that we're introducing ICD-10 in 2014. This will be a mammoth time of learning and mistake-making as providers and staff adjust to new, more detailed diagnoses code. This also will mean there will be significantly more access of patients records by people and providers on a daily basis.

Third, what would it cost us to provide such information to our patients? Since there is no solution that we have that is as simple as running a report and printing it out, we would have to train a person to look through three different systems, including our PM and EHR product and any other disclosures requested by the patient. I estimate the annual cost to train and maintain a person skilled enough to know clinical, billing and TPO disclosures would be about \$60,000. Frankly, this is not a sustainable cost for a small group. As you can understand, such accounting would be staff intensive and would be a significant administrative burden for our small group. Respondents to MGMA's questionnaire concur. If we were to provide that kind of accounting that is being suggested, the report would be extensive and we have no ability at this time to inform – to put the information in a suggested template. This and many other questions still need to be addressed by the regulation as it has been proposed and we hope to be able to address that in the questions that will be answered. Thank you so much for your time.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Thank you very much William, thank you for your time. We're – for the last presentation on this panel, we have Kevin Nicholson, who's the Vice President, Public Policy and Regulatory Affairs for the National Association of Chain Drug Stores. Kevin, are you ready?

Kevin Nicholson, RPh, JD – Vice President, Public Policy and Regulatory Affairs – National Association of Chain Drug Stores

Yes, thank you Deven.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Okay, terrific, may be just a little bit louder on your voice.

Kevin Nicholson, RPh, JD – Vice President, Public Policy and Regulatory Affairs – National Association of Chain Drug Stores

Okay, is that any better?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

That's much better, okay, you ready?

Kevin Nicholson, RPh, JD – Vice President, Public Policy and Regulatory Affairs – National Association of Chain Drug Stores

Sure.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

All right, go ahead.

Kevin Nicholson, RPh, JD – Vice President, Public Policy and Regulatory Affairs – National Association of Chain Drug Stores

Thanks again. So Deven, I wanted to thank you and the full Tiger Team and the full group for the opportunity to talk with you today about the perspective of chain pharmacy. NACDS members range from regional chain – regional pharmacy chains with four stores to national companies. Our members operate more than 41,000 pharmacies and employ more than 3.8 million employees. They fill over 2.7 billion prescriptions annually. As is discussed in other forums and by earlier presenters, the expansion of the accounting of disclosures requirement under the HITECH Act only applies to disclosures through an electronic health record.

It's important to note that an EHR is generated and maintained to give patients and as appropriate, others access to a patient's medical record. Just because health information is stored in or disclosed through a computer does not equate that computer system to an electronic health record. Notably, the HITECH Act provides grant funding for certain providers to adopt electronic health records and provides a mechanism for the development of criteria for determining the eligibility for such funding. Since not all healthcare providers are eligible for grant funding for the adoption of electronic health records, it is clear that Congress intended for certain providers to adopt a certain type of electronic health record and for specific requirements to attach to those records.

Pharmacies are not eligible for HITECH grant funding, consequently we believe that pharmacy computer systems are not electronic health records, as the term is defined in the HITECH Act. This logic is supported by the historical record of the HIPAA Privacy Rule. HHS recognized under the original HIPAA Privacy Rule that the additional information that would be gained from including treatment, payment and healthcare operations disclosures would not outweigh the added burdens on covered entities. Since most pharmacies are using substantially similar computer systems that they did when the original HIPAA Privacy Rule was finalized, HHS should reach the same conclusions with respect to the pharmacy computer systems now as they did in 2003. Furthermore, a quite important fact illustrates that individuals do not necessarily view pharmacy systems as EHRs, is that individuals have demonstrated little interest in their right to receive an accounting of disclosures.

Our member pharmacies who serve patients in almost every community across the nation have received each no requests or only a few requests each for an accounting of disclosures since the Accounting Rule became effective in 2003. Nevertheless, when an individual request is received, a significant investment of time and resources is typically required to respond to that request. Considering the billions of prescriptions that pharmacies dispense every year and the millions of patients served every year, and despite assertions to the contrary, our 10-year experience with HIPAA showed that only a fraction of a percent of Americans are interested in accounting of disclosures of their health information.

With respect to the proposed access report requirement, most pharmacy systems are not designed to track access at the individual record level, they do not capture the data elements being suggested. For most pharmacies it would most likely require a multimillion dollar project to invest in technologies that do not exist today. Moreover, we fear that an access report would inherently create a conflict with existing employee confidentiality and could result in misuse by a patient who may have a problem with a pharmacy employee, one that could be hostile or threatening.

For improper or unauthorized access to patient information, the patients already receive notification through the HIPAA Breach Rule or through the current Accounting of Disclosure requirements. If a situation rises to the level of a breach, the covered entity would be required to provide the patient with a breach notification. If the incident did not, the covered entity would log an accounting of disclosure, which would be made available to the patient upon request. Additionally, covered entities investigate complaints received from individuals, which produce a much better privacy result than an accounting, because it can address the root cause of the problem. And in a competitive marketplace that is patient service driven, any pharmacy that does not work with their patients, will find patients going elsewhere.

The technological and financial burden to implement a proposed access report far exceeds the benefits to the few patients who would request this type of report each year. In conclusion, we thank the Tiger Team for the opportunity to speak with you today. We believe that the expansion of Accounting of Disclosures requirement should apply only to disclosures made through an electronic health record as envisioned by the HITECH Act, and that the access report concept should be abandoned. An access report requirement would require pharmacies to adopt dramatic and expensive new systems with enormous financial, technical and administrative resources for a very limited and questionable patient interest. Thank you.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Okay, thanks very much Kevin. And with that, Paul Egerman, I'm going to rely on you to manage the question queue and just ask that you put me in it.

Paul Egerman – Businessman/Software Entrepreneur

Okay, so I will put you in it and I will tell the people on the computer system, if you can use the raise hand function if you would like to ask a question that would be very helpful. And if you're unable to access the computer system, you can just sort of break in and let me know and I'll put you in the queue. I will get to you in a minute, Deven. The first person in the queue that had his hand up for a very long time is Walter Suarez?

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

Oh, thank you so much, I feel like we are in Jeopardy, trying to push the –

Paul Egerman – Businessman/Software Entrepreneur

Yeah, well Walter, I left you hanging a long time on the last panel so I thought I'd give you first crack this time.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

Thank you. No, and I didn't know if I had raised it, or I kept it raised or – anyway, thank you I appreciate the opportunity. I do have two very quick questions. Thank you, first of all, for this great testimony. I think one of the most important points that came out of this in my mind is that the testimony is quite telling about the high level of trust the vast majority of consumers have in their providers when it comes to using their health information. I think the testimony really tells a very good story about that. I think we already have a number of regulations in place aimed at ensuring the privacy of health information is protected and we have new breach notification regulations. We have ways in which the patient can request an investigation or raise concerns.

And so my question – my first question is, what if instead of requiring all this extensive detail accounting of every instance of uses and disclosures and then provide that to consumers in many respects perhaps in a meaningless and confusing way. What if we were to enhance the ability and the mechanisms by which investigations are – of any perceived issue of inappropriate access are enhanced or improved. And so that was my question to the panel is, are there ways that you can think of or ways you can see these investigations, when a patient raises a concern about perceived issues about inappropriate access to their health information, can they be enhanced and conducted in a way that ultimately fulfills the goal we all agree on here and we're trying to address.

So that's a first question and the second question is really about a very critical term under the HITECH provision, which is "through an EHR." And this term has been and has created some confusion, and so I wonder if the testifiers can perhaps express what do they believe the meaning of "through an EHR" should be or is? How would you define "through an EHR?" For example, should it be limited to electronic data in a certified electronic health record system as defined in HITECH, or should it be inclusive of any health information about a patient that is maintained electronically? So those two questions, thank you.

Jutta Williams, CISSP, CISA, CIPP – Director, Corporate Compliance Privacy Office and Chief Privacy Officer – Intermountain Healthcare

So Walter, I'll jump in, this is Jutta from Intermountain. Thank you so much for asking the question. It's been our experience that providing a really in-depth investigation and answering questions has been pretty widely accepted by our patient community as being appropriate and what they are looking for. So enhancing on our already kind of robust investigative process at Intermountain would serve us insofar as we could maybe take a look at other systems and more data. But ultimately, it's kind of an individual human-to-human interview process that we have to rely on in order to answer questions about transparency because the systems can't derive context and we can't understand why an access event occurred to really derive whether it's appropriate or inappropriate, I don't know that technology is the answer to improving this experience. It's casting a wide net or casting a narrower net.

We need audit data to enhance our ability to conduct an investigation. And I think that there's an opportunity to clarify either through some sort of an interpretation of the Security Rule or potentially within Meaningful Use for certified medical electronic systems to provide really good, contextual in – or at least access information that we can then use to identify context. But by and large, the ability to conduct an in-depth interview is a people intensive process and so technology isn't going to enhance that so much. Maybe someone else has a different opinion.

Kevin Nicholson, RPh, JD – Vice President, Public Policy and Regulatory Affairs – National Association of Chain Drug Stores

This is Kevin with NACDS and I agree with Jutta. Our members already have in place very robust processes for investigating issues, complaints – when a patient has a complaint or when there's a suspected breach. And as Jutta mentioned, it's a very intensive process where there – it's a person-to-person process and it's hard for me to speculate at this point, but I can't imagine that there would be a technology that would improve upon that.

To answer your second question with respect to "through an electronic health record," it's our impression the HITECH Act set up a system where new – to incentivize healthcare providers to move toward a more robust systems, more interoperability. And to, through the meaningful use process, to set up criteria that providers would have to meet in order to be eligible for incentive funding. So in our view, the meaningful use process and the certified electronic medical process goes hand-in-hand with the enhanced accounting of disclosures requirement that was written into the HITECH Act.

William Henderson, FACMPE – Administrator – The Neurology Group, LLP (Albany, NY); Co-Chair, Board of Directors – Medical Group Management Association

This is Bill Henderson and I would respond to the second question as well. I pointed out that we have an integrated PM and EHR and frankly, the regulations speak about a designated record set. And even though I use the phrase EHR, the designated record set is what the definition goes by and that includes everything related to billing. And frankly, so much of what goes on to billing, inquiries back and forth between the insurer and office are all done electronically and they would need to include, I would assume they would be part of the record going back and forth between another entity in that entire process. So, I think we have to look at all those aspects or we have to narrow the definition. If we narrow the definition to what is truly an electronic health record, we'd have to be very careful to make sure it was specified with great clarity.

Lynne Thomas Gordon, MBA, RHIA, CAE, FACHE, FAHIMA – Chief Executive Officer – American Health Information Management Association

Hi, this is Lynn Thomas Gordon with AHIMA. In answering the first question, enhance investigations, I think as a healthcare provider, remember that the people working in the hospital or in the healthcare setting or at the doctor's office, we're patients, too. And we want to make sure if we're working in a doctor's office our coworker doesn't know what we had, I mean, we want our information to be private and secure. So I think that healthcare providers not only want to have the trust of the patients that they serve, but for their employees, they want to make sure that there's very robust investigations that are going on because as I tell people, I don't want anybody to know how much I weigh, much less if I have some terrible disease.

So I think that you can make sure that the investigations are really tied down. And we do everything we can as providers to make sure we know that our members do, to make sure that if anything has been breached or something, that there is a great forensic review and that efforts are taken to either penalize that employee up to termination. And then I think Bill did a nice job of talking a little bit about what the EHR means.

Paul Egerman – Businessman/Software Entrepreneur

Terrific.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

All right, thank you very much.

Jutta Williams, CISSP, CISA, CIPP – Director, Corporate Compliance Privacy Office and Chief Privacy Officer – Intermountain Healthcare

Oh, can I add one. This is Jutta again. Could I add one small item to my answer –

Paul Egerman – Businessman/Software Entrepreneur

Sure, go ahead Jutta.

Jutta Williams, CISSP, CISA, CIPP – Director, Corporate Compliance Privacy Office and Chief Privacy Officer – Intermountain Healthcare

– that's related to question number two. And for a designated record set system, I think there's an expectation that all designated record set systems are large and complex applications that can have an audit log attached to it. I want to emphasize that it's really any authoritative source used to make a clinical decision about a patient. And in some areas, those could be accessed database-based applications where if we're not careful in applying security rule changes or modifications to these sorts of systems, we could be asked to – or required really, to eliminate some really interesting and lifesaving systems from our environment.

For example, we have one small system used up at our primary Children's Hospital and because our physicians are all non-employed, it would be a disclosure every time it is used. It's a system that monitors brain waves for children during a very specific operation and it takes inputs from that surgery and gives outcome expectations based on clinical care – and that drives clinical care decisions. If you change the rule such that that designated record set now requires an audit log, we would have to remove it from our environment or completely replace it with new code. And so, just try not stifle innovation and clinical care best practice by applying a rule in an inappropriate way is my only ask.

Paul Egerman – Businessman/Software Entrepreneur

Great. Valuable comment, thank you very much Jutta. Thank you Walter for your questions. In the question queue right now I have Deven, Wes Rishel and Jack Burke. Go ahead Deven.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Okay, thanks very much Paul. I want to follow up a little bit on the conversation that started with Walter's question about providing patients with an investigation. What about a circumstance where the patient isn't satisfied with the investigation? Is there a role that an audit trail or some sort of log or report might be able to provide and either to bolster the investigation, which could frankly be beneficial for the provider as well as potentially the patient? And if that's the case, would that be a requirement or would that be something that would be an optionality, do you think, on the part of the provider? I think – we've written at CDT about the potential to have an investigation rather than giving patients reams and reams of data, but I'm worried about what happens if, in fact, the investigation isn't properly completed because the person that the patient suspects of getting in the record is someone powerful, for example.

And the other think that I would ask you all to comment on is, it sort of – I feel like when we got to this panel it almost became an us versus them dichotomy between what some of the patient groups requested in panel one and what some of the provider groups are reacting to here. So, some commentary on how we might be able to meet a little better in the middle, would also be helpful. Thanks.

William Henderson, FACMPE – Administrator – The Neurology Group, LLP (Albany, NY); Co-Chair, Board of Directors – Medical Group Management Association

This is Bill Henderson and I – if you listened to my initial comment, we actually in 2003 hired a part-time person whose job it is to explain patient's rights to them about access to health records, to talk with them in detail when they have questions about it. So I think, just looking at it from a practice perspective, I know that I'm not alone that there are practices who have made that kind of investment. I don't view it as an "us" versus "them" in any way because we value keeping the patient's privacy. We value them having access to the records, I don't think that's the question, I think the more pressing issue is, does the technology lend itself to it? Is it realistic to ask for all these things and what do patients actually want? If we don't clarify those points, then I think we're missing the boat on one of the more crucial things.

The other comment I want to make regards the matter of doing audits. I think that there's some potential for exploring the possibility. However, I would say if someone questioned an inappropriate release of their records or they – I can't imagine not doing that even though I don't have a completely satisfactory computerized audit tool at this time built into my software. I can't imagine not consulting whatever resources I had available, as well as talking to people who might be involved in it, as part of that investigation. So, I think you're going to make use of all of that in anything you're going to do because you have to do full and due diligence of any kind of request that's made.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Thank you, that's a very helpful answer. Does anybody else have any thoughts on that?

Kevin Nicholson, RPh, JD – Vice President, Public Policy and Regulatory Affairs – National Association of Chain Drug Stores

Deven this – go ahead. I would, this is Kevin with NACDS. I mean I agree as far as the audit process. Pharmacies are set up so that no one can access the patient record unless they sign in, they login, there's an audit trail that assigns access to every action that's being performed on behalf of the patient. So, there is an audit trail that is created and whenever – every time a prescription is filled, the steps along the process do record whether it was the pharmacist or the technician that performed that step. So that is used and that is useful and that is used when – in conducting an investigation to determine if something amiss had occurred. And then with respect to your comment about the "us" versus "them," I apologize if my testimony was perceived or was provided in sort of a defensive manner.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Oh no Kevin, it wasn't, it wasn't at all. I was just sort of – it was starting to look like some, although certainly not all of what the patients had asked for suggested in the first panel was being – that essentially that you guys pointed out a number of issues with it, which is a reason for the hearing, I mean we want to air all these things. But I'm just wondering if there's an opportunity also to sort of point out what some paths forward might be, that's all, you've – my apologies to the entire panel if I was – if it sounded like I was demeaning your responses. It's more I'm just trying to make sure that we address what might be possible as opposed to raising concerns about what's on the table.

Kevin Nicholson, RPh, JD – Vice President, Public Policy and Regulatory Affairs – National Association of Chain Drug Stores

I mean, we – I mean the pharmacies are extremely, extremely competitive. As you know, anyone who drives down any street in – any city street or suburban street will see, any of our member companies across the street from each other. So our members are very service driven and they do everything they can to make sure the patient is happy and is satisfied and wants to come back and be a regular customer. So, we feel that we are providing patients with the services and the information that they are – that they need and desire. And we're just – and I'm just providing you with the feedback from the – the honest feedback that I get from our members on what patients are asking for, in our – this is our perspective. This is what our patients are asking for, and it's not – they're not asking for these accounting of disclosures.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Yup.

Darren Lacey, JD – Chief Information Security Officer – Johns Hopkins University Health System

Yeah, as – this is Darren, Darren Lacey. A couple of things, one is, that with respect to areas where I think there's some mutual interest. I think it's, as a techie, I think it's great that folks are moving forward in terms of research and partial and maybe larger implementations of CCDAs products like – or tools like Blue Button, I mean, I think it's marvelous, I think it's great. And it goes to the other component which of it which is, that if we want to do a better job of investigating and a better job of detecting and a better job of basically covering lots of different systems and not just a few, then we need better logging standards. We just need – I mean audit logs need to have – I mean, there are some audit logging standards, there were some minimal standards in the access reports and HITSP has a few.

But I mean, I think we've spent, in the logging business, we've spent a long time working on CIS-Log. And folks like FairWarning and EPIC and Cerner could help, perhaps with the government's help, lead logging standards that most organizations – that vendors would be required to write to and that providers, like us or payers, would be able to actually extract meaningful, useful information. And also perhaps moving along, as we get better at this that would bead in to some of the things we're doing on CCDAs. I mean so I see all that coming around in this kind a nice sort of flow, it's just that the point some of us are making now is that it's a little early in that. The problems – the headwinds facing some of the things we want to do are stronger than most of us are comfortable with.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Yeah. Very helpful points, thank you.

Paul Eggerman – Businessman/Software Entrepreneur

Great, thank you. Next we have Wes, Wes Rishel? Wes, are you there?

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Yes, I'm here. Thank you. So, we had a comment during testimony relying on the cost impact analysis in a 2003 rule as evidence about the costs of this proposal. And I would just like to make a counter comment that the cost impact analysis and rules have not historically been good predictors of the cost of implementation. And furthermore, in another 10 years we probably understand the issues a lot better than they did back then. And that leads to my question to Jutta, you mentioned a \$100 million cost estimate and I think that that was surprising to folks and I wonder if you could, given a few more minutes here, you could help us understand how you reached that estimate? And then finally, I just want to comment on Deven's question was great and that I think I hear two possible trends developing. One is sequencing the ability of consumers to get this information over a longer period time so that it fits into the replacement cycle of systems. And two, possibly other areas of recourse if the response from a provider isn't acceptable to the patient. So Jutta, you help us understand your costs?

Jutta Williams, CISSP, CISA, CIPP – Director, Corporate Compliance Privacy Office and Chief Privacy Officer – Intermountain Healthcare

Happily, thank you. I wanted to make – say thanks for the question Deven and also for the check. I wanted to emphasize, too, that at Intermountain patients are center to everything that I do for my job and that Intermountain is patient-focused and always has been. And so it was a little bit surprising to hear there was kind of a tone of “us” versus “them.” I genuinely feel like my office is a patient advocacy office and that’s why we report directly to our board and not up to our business. So if that came across, then I apologize very much.

To answer your question though, when the first – when we had an RFI on the subject of accounting of disclosures back in 2010, we did quite a bit of calculation on what it would cost just to implement the rule for treatment, payment and health care operations for disclosures. And what we found is, we have a lot of systems that are doing automated disclosure and reporting to state agencies and to other organizations through queries and not necessarily through direct patient access. So in order for us to invest in technologies that could kind of watch the stream of data that was being prepared and sent through interfaces, it actually required quite a lot of technical development in order to sift out patient record disclosures through that sort of an interface.

So we had invested I think almost \$2 million on one particular interface in developing the capability to monitor which patient records specifically were going through the interface for a state reporting requirement in the state of Utah. So that was one of many interfaces that we had to develop. And so when we saw the access report come through a little under a year later, we look at all of the applications that we would consider inside of a designated record set and we said, okay, which ones of these actually have the capacity to provide an inquiry audit log, and the number was relatively low. Software product vendors, and a lot of these are legacy systems that have been around for many years, we don’t replace our systems on a two or three year basis. We have some systems that have been in place for 20 and 30 years, especially on our billing side, where AF400 systems just run really efficiently and we don’t replace them very frequently.

So for some of our applications, and especially the more modern ones, we went to the vendors and said, hey, if we needed to have a reader-inquiry level audit capability, where we can attach a user to a specific record, how would you go about doing that, where would you put it in your product lifecycle? And most of the application vendors in this space are working on a lot of other different things. And in order for them to put something like this in their development lifecycle, and I think we heard this from a couple of our technology vendors earlier today, they had to weigh that requirement against many other competing interests, especially around meaningful use accreditation or attestation. So one particular vendor, which is a large claims-management vendor on our payer side, suggested it would be a \$3 million cost for them to apply consulting dollars against that particular product to develop a read-inquiry audit. And we said, \$3 million dollars per application, that’s pretty substantial. That might not be for every one of the applications in our designated record set, but it could be indicative of that.

So we took a look at which of those systems could even be upgraded such that we could code the ability to provide a read-inquiry audit and we found that a number of them couldn’t. And we would actually have to replace some applications in order for us to be able to deliver an access report as conceived in the NPRM. So that’s where the numbers came from. And it wasn’t just us who came up with those numbers. During the comment period, a number of letters were received by OCR from other very large organizations, like ours, that are early adopters of technology and have the ability to really calculate these costs and understand what would be required, and the numbers came back staggering across the board. I know that Kaiser, and maybe Walter could speak to it, Kaiser came up with some very substantial numbers as well, as did our friends at Mayo. And we’ve all been kind of coming out to DC and trying to express concern for probably the last two and a half, three years. So that’s where a lot of the numbers come from.

In addition you have to invest in technologies, kind of like what Kurt was describing as is FairWarning, which is that aggregation and correlation capability that consumes the data that these underlying applications would be producing. And so there’s an investment cost there as well.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Thanks. Finally, you've made a statement and I've sort of independently investigated it, but I just want you're testifying here. Are you aware of any country that has a requirement to disclose staff members to patients outside of a court discovery process or something, or any other industry in any other country that has that kind of requirement?

Jutta Williams, CISSP, CISA, CIPP – Director, Corporate Compliance Privacy Office and Chief Privacy Officer – Intermountain Healthcare

I'm not an industry expert for international privacy law and I've only looked at what I know from industries here in the United States. And I did risk assessment work for one of the big four in a number of different industries and in my personal experience, I did not see any other industry that had this level of transparency requirement. It's effectively like asking to walk into a bank and say, hello, I would like to have a copy of anyone who's ever seen my credit balance and my account number at your bank. This is far in excess of what is required by fair credit reporting, in principle, and so to ask for individuals by name to my knowledge is not required by any other industry.

Kurt Long, MS – Founder and Chief Operating Officer – FairWarning, Inc.

Hey, this is Kurt Long, and may I comment on the international aspect of access reports, I have some information to share?

Paul Egerman – Businessman/Software Entrepreneur

That would be very helpful, go ahead Kurt.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Please do.

Kurt Long, MS – Founder and Chief Operating Officer – FairWarning, Inc.

Yeah, with NHS Scotland, for the entire country, it's on a relatively small-scale for a country, the 5 million citizen patients, they have moved forward with broad scale access reports for health information exchanges as well as an access report toward patients. And then in all of England, within the last 60 days, Jeremy Hunt, their Minister of Health together with Dame Fiona Caldicott did pass Dame Fiona's recommendations to provide for an access report for everyone, in what is now called NHS England. And even though the passage of that law is well-intentioned and it's helpful for us, the technical obstacles still remain. Nonetheless, they did in fact pass these rules based on Dame Fiona's findings.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

And was that for – or –

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Just to be clear, I think it's important to distinguish between requirements that have been stated and requirements that have been fulfilled. And I guess I was really asking the question, are we aware of any place where there's system in place to do this.

Paul Egerman – Businessman/Software Entrepreneur

Yeah, so that's a great question, Wes. So I understand what you're saying Kurt, there are perhaps some rules or some laws that may have been passed but are not yet operational, is that – or is that not right?

Kurt Long, MS – Founder and Chief Operating Officer – FairWarning, Inc.

Yes. And I want to add a little bit of a positive element, because I do spend a lot of time in Europe, Canada and the United Kingdom serving our customers. And I do want to add one positive element, I've been amazed at the level of expertise that the United States has in the area of legal expertise in being able to craft legislation. And like – whether you like it or don't like it, meaningful use as well as very specific laws that get negotiated and passed, the level of detail that we're at in a prescription is well ahead of the markets that we visit, which are generally, when you see the passage of these kinds –

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Kurt?

Paul Egerman – Businessman/Software Entrepreneur

That's helpful.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

It's a really important point to made and Kurt, thank you for helping us out on this panel.

Paul Egerman – Businessman/Software Entrepreneur

That's right –

Jutta Williams, CISSP, CISA, CIPP – Director, Corporate Compliance Privacy Office and Chief Privacy Officer – Intermountain Healthcare

It's that Security Rule is a very different animal than any of the data processing laws in Europe and we don't have the same ability to rely on supplier law to require the delivery of those audit logs. And so we don't have that building block necessity to build an administrative program on that we can then attach a patient privacy right to. And so we don't have the underpinning technological requirement the way they do in data processing laws in Europe and so I just wanted to emphasize that point and maybe we can move on.

Paul Egerman – Businessman/Software Entrepreneur

Terrific. So great question Wes. Thank you Kurt, thank you Jutta for your helpful comments on cost and the helpful discussion on what is currently operational outside the United States. I have Jack Burke in the queue? Jack, are you there.

John J. Burke, MBA, MSPHarm –Vice President, Corporate Privacy Programs – Harvard Pilgrim Healthcare, Inc.; NCVHS

Yes I am, can you hear me?

Paul Egerman – Businessman/Software Entrepreneur

Yes.

John J. Burke, MBA, MSPHarm –Vice President, Corporate Privacy Programs – Harvard Pilgrim Healthcare, Inc.; NCVHS

Great, this is a question perhaps mostly for Jutta and Bill, but anyone else on the panel, and thank you all the panel participants for your contributions. My question goes to whether or not as a result of some internal investigation an employee has been discovered to have been committed some misstep, which results in an exposure of information, not rising to the level of a breach where concurrent notification to the individual is expected, but nonetheless an accounting of disclosures should be filed. Do any of you have experience with the effects on an individual of you reaching out to that affected person and informing them of what has occurred? This goes towards a little bit of meeting in the middle that we talked about, whereas we're not required to necessarily notify nor are we prohibited from doing that.

Jutta Williams, CISSP, CISA, CIPP – Director, Corporate Compliance Privacy Office and Chief Privacy Officer – Intermountain Healthcare

So I have a lot of experience with this because we get to sign all the breach letters out of my office, so I'm essentially oversight for all of our investigations. And infractions run the gambit, they can be everything from a person making a mistake in stuffing an envelope inappropriately or handing the wrong instructions to the patient, all the way up to malicious acts. And so you're right, not everything is a reportable breach. Everything that is identified as a breach, though, is reportable under current accounting of disclosures rules. So if we do identify something inappropriate happened and there is no breach notification letter because it didn't rise to that level, it is included in an accounting of disclosures report. So a patient would have the right to know about that disclosure – that that really inappropriate use that didn't result in what we call an inappropriate access or disclosure, shows up in that report.

I talk to patients almost every day and I'll tell you, on occasion, and it's hard to identify patients who would come and be public in their experience. I did reach out to a few, seeing if they would come and talk about their experience. A vast majority of them are so relieved, just to have a conversation about that did happen that this did happen, we took the appropriate action, an employee was sanctioned or an employee wasn't, sometimes it's re-education and training or a process improvement. And patients, when they understand that you took their concern seriously, and that you took a reasonable and appropriate response to their concern or their experience, are really satisfied with that as a result. And if they aren't, if they feel like we aren't taking the appropriate action, that we haven't taken their concern seriously or that our process is broken, they have recourse.

And in our Notice of Privacy Practices, we talk about that recourse they can go to OCR. And even though the OCR, and I appreciated this perspective that was given to me a few weeks ago. The OCR is not a customer service ombudsman for patients, they are the organization that is supposed to evaluate me and my program and make sure that I have the appropriate process in place to investigate complaints and that patients are getting a fair treatment under that investigative process. So in my opinion, it runs the gambit, it usually requires a conversation with the employee involved, it usually requires a conversation with the patient involved, technology is an enabler, but technology is not the solution.

John J. Burke, MBA, MSPHarm –Vice President, Corporate Privacy Programs – Harvard Pilgrim Healthcare, Inc.: NCVHS

Thank you.

Paul Egerman – Businessman/Software Entrepreneur

Great. Thank you. And is there anybody else who would like to ask –

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Paul, I – this is Leslie. I've had my –

Gayle Harrell, MA – Florida State Representative – Florida State Legislator

Gayle would like a question, too please.

Paul Egerman – Businessman/Software Entrepreneur

Yeah, go ahead Leslie.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

So it's hard to know what to make of the fact that you don't get more requests. It may be that patients simply are unaware of what actually goes on, and how the information might be beneficial to them and so on. And several of you suggested as an alternative, relying on the internal processes that you have in place and I wonder what your views would be about making that alternative more robust by, for example, not indicating to people, individual employees, but publishing statistics about the numbers of investigations. The numbers of claims closed, the numbers of breaches, numbers of the individuals involved in breaches or publishing much more detailed information about your various efforts to protect patients, so that patients could actually compare providers in terms of what they're doing behind the scenes.

Jutta Williams – Director, Corporate Compliance Privacy Office and Chief Privacy Officer – Intermountain Healthcare

That's a really interesting idea Leslie, one I hadn't really considered before, like a star rating or some sort of a scorecard that patients could use to understand kind of our privacy practices as an organization is an interesting idea. There is a bit of an interesting side effect when you have a really robust program. We investigate a lot of incidences, because we do a lot of education with workforce members and frankly with our patients as well. And so we have more reports than average because we have an educated population that we're working with. When we reported all of our metrics, because we're structured very differently than a lot of healthcare companies where one legal entity for all the health services organizations. When we reported to HHS about our breach notification process each year, there was an alarming response that said, how you could you possibly have that many incidences as one organization.

And so I agree that a scorecard would be great in percentage basis or even a star rating would be fine, but if we had to report numbers, it would have a chilling and cooling effect on any kind of proactive program we would put in place, because reporting the numbers will raise concerns. And so I just would want to explore how to do that in a balanced way so it doesn't kind of affect how proactively people will apply privacy principles and best practice. And we don't want people to stop looking proactively for inappropriate access.

William Henderson, FACMPE – Administrator – The Neurology Group, LLP (Albany, NY); Co-Chair, Board of Directors – Medical Group Management Association

This is Bill Henderson, I'd just like to make a little side point in this and I think it points to a need that we all have. We're in the process of rolling out a patient portal in which our patients, as many around the country can do, can have access to their reports to see the details of their laboratory results and the like. And I'm stunned that in spite of efforts to encourage people not only to sign up and make use of the portal, but actually to access it, to understand what records are being kept, just by our practice, that there is relatively little interest in doing that. And so I think we owe it to the public in general, just because we are patient-centered to let them know that this opportunity and resource exists for them as part of that process. I think then the issues that – some of the issues we're talking about that relate to disclosure and breaches and the like, and how we investigate those and detail those will make much more sense to patients in general. So that's just a little side point, but I think we need to remember that.

Lynne Thomas Gordon, MBA, RHIA, CAE, FACHE, FAHIMA – Chief Executive Officer – American Health Information Management Association

This is Lynne Thomas Gordon from AHIMA. I'd just like to second that. I think our patients, maybe one of the reasons we don't get as many requests is they're just learning that if they partner with their providers and learn more about what's going on with their healthcare, they will be a better patient, or if there is a loved one of the patient, to really know what's going on. We personally are trying very hard to get people to learn about their personal health records and the importance of having that information, whether it is for your use here or you're traveling. And we're monitoring how many people go to our website on MyPHR just to see, can we get that word out and how we work with our 67,000 members to really go to their churches, synagogues, schools, etcetera to encourage people to understand their personal health record better. So I think that as people get more familiar with that, perhaps the request for who else is seeing their record will go up. Thank you.

Kevin Nicholson, RPh, JD – Vice President, Public Policy and Regulatory Affairs – National Association of Chain Drug Stores

This is Kevin with NACDS and I would like to echo a comment that Jutta made, and our members range from very, very large companies with thousands of locations to some very small chains that have just fewer than 10 locations, so, I think that's an interesting concept, the scorecard. We are seeing that in other aspects as Jutta mentioned with star ratings, and I think there is a move in health care generally towards more transparency. And so that type of scorecard concept and quality rating concept, I think it is interesting, it may be worth exploration. But again, I think Jutta makes a very good point, that a larger entity or an entity that is perhaps doing a better job may actually look worse because of the fact that they have a better system in place and that they're just a bigger entity.

Paul Egerman – Businessman/Software Entrepreneur

Um hmm.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

So Paul, it's Deven. I know we're sort of creeping up to the end of this panel, but I heard Gayle's voice and she hasn't had a chance to ask a question. Would you be amenable to extending this question and answer period just a little bit more, given that our payer perspective panel is a little smaller.

Paul Egerman – Businessman/Software Entrepreneur

Sure, go ahead Gayle.

Gayle Harrell, MA – Florida State Representative – Florida State Legislator

Hey, thank you so much. I just wanted to ask one specific question because I'm a little concerned, as Deven was, with this "them" and "us" kind of the mentality that's somewhat evolved and that I certainly don't want it to get to that point. I think we need to start thinking a little bit more out-of-the-box on how to really implement – really making this information available to patients. And they have a great deal of concern on privacy and security matters, there's no doubt about that. And as we move forward, one of the things I would like us to do is to really do that thinking out-of-the-box and ask all of our panel discussion members to come back with us with the one concrete thing that they would do. It's not going to cost \$100 million dollars, it's not going to be so intrusive and impossible to do, what's the one concrete thing – I'd like just – people now, just to say one concrete thing very quickly.

Lynne Thomas Gordon, MBA, RHIA, CAE, FACHE, FAHIMA – Chief Executive Officer – American Health Information Management Association

Lynne Thomas Gordon, AHIMA, I think we need to do a better job of educating our patients, a lot of it's just patient education.

Jutta Williams, CISSP, CISA, CIPP – Director, Corporate Compliance Privacy Office and Chief Privacy Officer – Intermountain Healthcare

This is Jutta from Intermountain. I would really like to understand exactly what transparency need that there is so that we can develop a specific requirement to it. I've heard one use case that actually made really good sense to me when I was speaking with one of the advocates recently. And that was, transparency about when a record is requested outside of an OHCA, outside of a routine use and disclosure within the organization by physician or payer that we have no knowledge really has a true relationship with a patient. And the recommendation was – **3:58:18-27** that way when there's no human interaction with the person requesting a record, that they're requesting it entirely through electronic means and then there's no authorization required.

My challenge sometimes though is just understanding what exactly the transparency need is because genuinely, I want to develop against those requirements, I want to provide patients better service. And until I get a specific request and a specific case study that we can develop against, it's hard to develop a technical recommendation. Vague notions of transparency are challenging for me to develop against and I think that OCR tried to do that with access report and we found not understanding what was specifically needed resulted in a response that was not going to address the need. So a specific requirement would be great, I would be happy to develop against that if it were this particular use case, then let's require access logs for inquiry requests for records through the Direct model for meaningful use certified systems.

William Henderson, FACMPE – Administrator – The Neurology Group, LLP (Albany, NY); Co-Chair, Board of Directors – Medical Group Management Association

This is Bill Henderson. I guess I would affirm and second what Lynne said. I think the message for education though, I wouldn't take it so simplis – I mean, not that Lynne said anything that would be like this. But I think many voices coming from many perspectives, from patient advocate perspectives, from physician perspectives, from health system perspectives to instill upon people the importance of them knowing about their medical records and the rights that would be critical. I think more messaging across many platforms will make a better and informed patient population.

Kevin Nicholson, RPh, JD – Vice President, Public Policy and Regulatory Affairs – National Association of Chain Drug Stores

This is Kevin with NACDS and again with respect to having a more informed or a better informed patient population, I – and it's sort of to kind of pull in some of the comments made by my fellow panelists. I think we would like a better understanding of the need. I mean, I imagine it is – we – I imagine it is a need for more transparency for better understanding for the practices of healthcare providers, of covered entities, of business associates, etcetera. So if there is a way of doing that similar to, again like the – some sort of quality measure, I think that is an interesting concept that is worth exploring.

William Henderson, FACMPE – Administrator – The Neurology Group, LLP (Albany, NY); Co-Chair, Board of Directors – Medical Group Management Association

This is Bill again, just one other point. I think that, to speak to Kevin's point, too, we have to have more dialogue between all the parties, which include physicians, Office of Civil Rights, ONC and the like to really – to come together to pilot something so we can all look at how these can interface and work well together. I think we might find success along those lines.

Paul Eggerman – Businessman/Software Entrepreneur

Very helpful comments. That was a great question Gayle. So, let me just take a second to say thank you to our panelists for presenting valuable information. It's unfortunate we do this over the phone, but I want to make sure you know how sincerely appreciative Deven and I and all of the members of the various committees are of your efforts. So, thank you so much. And Deven, are we ready to transition to the payer panel?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

I think we are Dixie, are you ready to take us through?

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates

Yes, I am.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Okay. Well you can go ahead and introduce your first panelist and I'll continue to keep your time.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates

Sure, thank you. I do want to point out at the outset that unfortunately I'm not able to join the –

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Oh, you're not on either.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates

No, and I'll just say, I guess not enough people have dropped off to allow me in so I'll follow Deven's lead here and Paul, if you could, when we finish here giving the testimony, I'll ask you to handle the Q&A and commend you for how well you did it for Deven.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

You're pulling –

Paul Eggerman – Businessman/Software Entrepreneur

Thank you, I think. Happy to help.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates

Yeah, thanks. I'd like to thank – we have two presenters for the payer perspectives panel, this is the last panel of the day and I'd like to start out by thanking both of these presenters for participating in this hearing today. Again, with this panel, although we only have two presenters, each of these will follow the same format, each presenter will be given five minutes to provide testimony. And as with the other panels, the rooster will crow when there is one minute left –

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

No, just 30 seconds, Dixie.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates

Oh, 30 seconds left, felt like a minute. And once you hear the rooster, I would appreciate it if you try to come to a conclusion within the 30 seconds remaining. After both testimonies have been given, we'll have a 40-minute period of Q&A. The two individuals who are participating representing the payers today are Scott Morgan, who is the Executive Director and National Privacy and Security Compliance Officer for the Kaiser Foundation Health Plan. And Jay Schwitzgebel who is the Director of Information Security and IT Compliance for CareSource. And thank you both for participating. Scott?

Scott Morgan, MPH - Executive Director and National Privacy and Security Compliance Officer - Kaiser Foundation Health Plan, Inc.

Thank you. The Kaiser Permanente Medical Care Program is a large integrated healthcare delivery system and includes regional health plans as well as medical groups and hospitals. We've made a significant investment in a secure electronic health record system. To frame our comments, we look to HITECH's balancing test that considers both the interests of individuals in learning about disclosures and the administrative burdens on covered entities that must account for disclosures. In our experience, very few individuals request accounting, when they do they rarely request health plan disclosures. They also focus on specific concerns, not a broad accounting. The added benefits to consumers are small compared to the high costs to automate treatment, payment and health care operations or TPO disclosures and access reports. Like Intermountain, we estimate the cost to be, for only one of our eight regions, would exceed HHS estimates of the total cost for all covered entities in all states.

One of the goals of this hearing is to gain greater understanding about currently available, affordable technology. Kaiser Permanente has already implemented robust tools to respond to requests from members and patients about their records. Strong access controls ensure that only authorized individuals can access PHI. Alert systems monitor for and record inappropriate access. We've instituted various other deterrent mechanisms including physical, technical, administrative and policy safeguards. Additional system capabilities to track internal uses of PHI would not lead to justifiable improvements or greater transparency.

Another goal of this hearing is greater understanding about how covered entities and business associates currently deploy access transparency technologies. We agree that individuals should be able to ensure their PHI is not accessed inappropriately, but we believe the proposed access report is not the right solution. Access reports could result in less, not more transparency, because critical information can be buried within large amounts of data. Also, underlying technology such as a system audit log is not designed to provide usable information for patients and would require significant redesign and upgrade to produce an access report. There are more effective, less expensive methods to respond to privacy concerns.

An investigation by the covered entity can yield more detailed, reliable and responsive information in a proper context at a lower cost. Even for a targeted inquiry, lengthy reports may surprise, confuse and overwhelm the consumer and erode the trust relationship between patient and provider. Typical access logs we've provided run 60 to 100 pages, but reports from inpatient logs can exceed 1000 pages. Patients do not recognize most of the names on the report, and there can be several dozen names, especially for hospitalizations. We recommend investigation as an effective alternative to an automated access report.

We also want to address certain uses, access and disclosures in an integrated system. Our integrated model includes health plans, clinicians, inpatient and ambulatory facilities, laboratories and pharmacies as well as research centers. In each Kaiser Permanente region, different legal entities participate in an organized health care arrangement or OHCA. Under HIPAA, PHI exchanges between OHCA participants are considered disclosures, not uses. Kaiser Permanente entities routinely share high volumes of PHI to support various joint activities including and especially TPO, for example, between health plans and hospitals or between hospitals and medical groups. As an integrated model, much PHI resides on many IT systems shared by our OHCA participants and within the scope of the proposed rules. Access to PHI in these systems looks more like a use than a disclosure. We believe that excluding these technical disclosures from an accounting would not raise any genuine issue of privacy. Individuals expect integrated entities to share PHI as outlined in the OHCA's shared Notice of Privacy Practices.

In summary, we have the following recommendations. Focus regulations of the requirements for accounting of disclosures in the HITECH statute and do not require access reports. And exempt TPO disclosures between covered entities within organized health care arrangements. Thank you to the Tiger Team for the opportunity to participate. I'd be happy to respond to any questions. No rooster?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

You did well you beat the rooster.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates

Yes, very well, Scott. Thank you –

M

And we thank you for that.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates

Thank you very much.

Scott Morgan, MPH – Executive Director and National Privacy and Security Compliance Officer – Kaiser Foundation Health Plan, Inc.

Thank you.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates

Our next presenter is Jay Schwitzgebel. Jay?

Jay Schwitzgebel, CISM, CISSP-ISSMP – Director of Information Security and IT Compliance – CareSource

Thank you Ms. McGraw and distinguished members of the Office of the National Coordinator's Privacy & Security Tiger Team. I'm Jay Schwitzgebel, I thank you for allowing me the opportunity to present my views about the HIPAA and HITECH Act requirement. I am testifying today on behalf of CareSource and AHIP. CareSource is an independent, nonprofit Medicaid managed care organization headquartered in Dayton, Ohio. As one of the largest Medicaid managed care plans in the country, we provide specialized care management for some of the communities most vulnerable citizens in Ohio and (Indiscernible). We're also member of the National Health Insurance Association, America's Health Insurance Plan, whose members health and supplemental benefits cover more than 200 million Americans.

Overall, I'd like to make four main points. As we engage consumers in new marketplaces for state and federal exchanges, and new program models for Medicaid, plans such as CareSource are open to exploring new ways to make pertinent information available to consumers. Any new proposals should first precisely identify consumer the need before further steps are taken by federal regulators or advisory bodies. Second, evaluate ways to enhance transparency for consumers using a reasonable cost-benefit analysis that avoids unnecessarily prescriptive and costly requirements. Third, follow congressional intent for the HITECH Act requirements and fourth, be coordinated in the pertinent federal agencies to effectuate consistent privacy and security policies across federal programs, while retaining OCRs authority and primary responsibility for the HIPAA and HITECH regulations.

There are different agencies and advisory bodies participating today that have different jurisdictional responsibilities and objectives. We all share the same goals, keeping the availability of consumer's health information available for their healthcare and assuring that consumers understand and trust in the processes we utilize to protect the privacy and security of health information. We urge all federal partners to stay abreast of each other's work and encourage the HHS Office of Civil Rights to maintain the integrity of oversight for interpreting and promulgating HIPAA and HITECH Act requirements. In the rest of my time, I'd like to illustrate the reasoning behind these key points as the person responsible for HIPAA and HITECH compliance activities within my organization.

More frequently when health insurance plans consider methods to increase transparency for consumers and access to electronic information, it's within the context of new benefits and processes designed by health insurance plans to serve consumer needs, such as platforms available 24/7 to enable online access to personal account information. And online access to programs that further national goals to promote healthy lifestyles or align with management of chronic disease. At CareSource we serve nearly 1 million consumers and since the accounting of disclosures requirement became effective in 2003, our privacy office has not received any consumer request for this report.

In my opinion as an IT professional, developing and implementing an access report may actually cause consumers unwarranted concern by using overwhelming volumes of routine information without achieving information transparency. These reports were not required by the HITECH Act and there are better ways to make pertinent information available to consumers. We encourage HHS and related agencies to build on this hearing, precisely identify any consumer needs and then develop federally funded contracts or grant award programs to which consumer studies can be undertaken to identify and define what consumers believe they need in EHRs, as well as from HIPAA covered entities.

It's been our experience that our members want to see their healthcare dollars spent wisely. We all understand that electronic technologies can change over time and health entities should leverage new processes and solutions to make improvements that keep pace with consumer's expectations. In the case of a proposed access report, we expect that it would cost millions if not billions of healthcare dollars to implement and that very few consumers would request it. These facts do not justify such a costly investment. Additionally the HITECH Act Accounting of Disclosures statutory provisions were tailored to clinically-based electronic health record systems that are primarily designed to support the treatment of patients, that enable better record-keeping and use of the health information. These provisions were implemented to compliment the corresponding incentive program that was established to provide monetary incentives to providers to adopt EHRs and allow for meaningful use of these applications in a clinical setting.

At CareSource we do not have electronic health records as defined by – and therefore are not eligible for the incentive payments. CareSource employees a state of the art claims management system, but it's not designed to provide the detailed logs that would be required under federal proposals nor can it be trivially adapted to do so. Federal actions should conform to the purpose outlined by Congress in the HITECH statute initially, rather than require broad new and sweeping changes across all HIPAA covered entities. As I hope my testimony has explained, we are committed to leveraging electronic technologies to enable consumers access to information and providing them with the information that they need in a private and secure manner. Thank you all for allowing me the opportunity to express my views and experiences.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates

Thank you. Thank you both for your testimony. I still can't access – I don't know who has questions so Paul, would you please –

Paul Egerman – Businessman/Software Entrepreneur

Yeah, Dixie, I'll be happy to handle that for you. People should raise their hand on the screens if they would like to ask questions or just, like Dixie, a few of the people were unable to get on, just somehow call out your name or send me an email or something, and I'll make sure I put you in the queue. We have Peter Kaufman has his hand raised.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

I'm trying to organize my question a little bit better, can you pass and put me in a couple later, just –

Paul Egerman – Businessman/Software Entrepreneur

Okay, right now, you're the only person in the queue. Is there anybody else who would like to ask a question?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Sure, I'll ask Paul, it's Deven. So what I'm interested in hearing, one of the points that Kevin Nicholson brought up in his testimony and the previous panel was suggesting what Congress intended in HITECH was a focus on accounting of disclosures from EHRs, which is in fact the language that's in the HITECH legislation. And he posited that in fact there was never an intent to reach beyond the EHRs that were part of the meaningful use program, and I may be putting words in his mouth, but that was generally the gist I got. And so I was actually somewhat surprised that neither one of you, unless I missed it, was suggesting that in fact that payers should be excluded from any sort of resolution of this and instead you were suggesting that there's some – a role of transparency from the payer and that certainly what's been proposed is not workable from your standpoint. So I'm wondering if you would comment on that aspect, if you care to and sort of what elements of sort of providing patients with a greater understanding of who's accessed their records, such as in the case of a suspected inappropriate access that payers would and could or should be doing for their patients?

Scott Morgan, MPH – Executive Director and National Privacy and Security Compliance Officer – Kaiser Foundation Health Plan, Inc.

Well, okay, this is Scott. You're right, I did not call out that payers should be excluded, but that does seem to go along with the original scope. We were proposing to return to the original scope of the HITECH statute and my understanding that there would not be an EHR at a payer. So it would kind of automatically take out the payers.

Jay Schwitzgebel, CISM, CISSP-ISSMP – Director of Information Security and IT Compliance – CareSource

So this is Jay –

Scott Morgan, MPH – Executive Director and National Privacy and Security Compliance Officer – Kaiser Foundation Health Plan, Inc.

Jay, do you want to add to that?

Jay Schwitzgebel, CISM, CISSP-ISSMP – Director of Information Security and IT Compliance – CareSource

Yeah, I mean, I would agree with what Scott said. I mean, the traditional EHR is not in use at CareSource and the payer, I mean, we're looking all internally. So the inquiries we might get, or the requests we might get from a member would be about disclosures internally that are within – covered by TPO unless there were an abuse. So the work that I do in the security team is to investigate something that we may find through our existing security monitoring or even an inquiry we might get from a member, but it's inconsistent with providing a record or report of those disclosures to the actual member. Because as we've been hearing all day long, any sort of an automated log off that kind of data is going to be filled with – overwhelmingly the majority of those accesses are going to be non-human, they're going to be systems-based accesses that are just impossible to be meaningful to the outside consumer.

So I don't know if I directly answered your question, but I recognize a need to be forthright. We certainly are member focused and we don't want to leave anybody feeling like that somehow we're being opaque, but I absolutely believe there has to be the human involvement in the investigation that happens in the back-end before we could divulge any sort of automated record of those logs.

Scott Morgan, MPH – Executive Director and National Privacy and Security Compliance Officer – Kaiser Foundation Health Plan, Inc.

Yeah, I would agree, just one more, because you asked us that other question, Deven, that again, it would be that we have tools where logs exist to do the investigations when our members have questions or concerns. As well as the usual, they can access the record through the access to PHI right under HIPAA and be notified of any type of breach.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Okay. That's really helpful to know, I mean, just for the record, I'm not – I don't necessarily agree with an interpretation that the EHR language in the statute is limited to provider EHRs. And in particular those that are certified through the Meaningful Use Program, if only because there are lots of provisions in the HITECH privacy pieces that frankly are not limited to the Meaningful Use Program. But given that the question was raised, I wanted to give you both a chance to answer it, as well as to sort of reflect on what payers might do from a transparency standpoint, particularly when there's inappropriate access that's been alleged, either by a member or by someone else. So, that's helpful to know. Umm – .

Paul Egerman – Businessman/Software Entrepreneur

I'm sorry, were you done Deven?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Yeah, no, I am.

Paul Egerman – Businessman/Software Entrepreneur

Because I had – I was – I didn't quite understand your comment Scott, because I looked at Kaiser and it's hard to know where you're EHR system ends and your payer systems begin. And so my question is, well, isn't all from a patient's perspective, doesn't Kaiser just have an EHR system?

Scott Morgan, MPH – Executive Director and National Privacy and Security Compliance Officer – Kaiser Foundation Health Plan, Inc.

Kaiser does, but we have several – many important systems that would be considered payer, non-EHR systems. And that's part of what, to reflect a little bit on what Jutta from Intermountain was describing in how to – their cost looked so high, we face – we do face a similar type of review, if you include all of the systems that could be in scope, and there are many beyond EHRs.

Paul Egerman – Businessman/Software Entrepreneur

Well, that's right, but even an organization like Intermountain Healthcare or Johns Hopkins has non-EHR applications. They might have a credit and collections application that sends out credit letters, for example, it's not really an EHR, but one would expect that to be included and so, I view it as a challenge to try to define where EHR stops and payers begin. Let me see if people have questions. Peter Kaufman you have your hand back up and Deven has her hand back up also?

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

I guess I didn't realize it had gone down. I believe we've heard clearly that providing full reports of access and disclosure may – full reports may be expensive and complicated and possibly dangerous for staff, something I wouldn't have thought about. And that it's possible patients are only rarely interested in that anyway, and if given the choice between one or the other, would likely prefer other EHR enhancements like health maintenance features over a full and complete auditing of who touched their record and who accessed it. That's not saying that's not something that should be available, but given the other features, it may be something that we want to hold off on a little bit.

But more importantly, in my opinion as a physician, healthcare works better when there's an inherent trust between the provider and patient rather than when based on the patient keeping track of everything the provider is doing because they don't trust the provider without that. And I hope the government and private groups can realize that the trust is an issue and while scrutiny should be possible, perhaps it shouldn't be encouraged through fear. I know this may be a controversial and inflammatory statement, but it's one of those things that as a provider, I worry about maintaining trust with my patients. And it's been harder during the course of my practice, which has spanned only 25 years – well 28 years if you consider my academic time, to see the difference in how patients view their doctors and calling them providers instead of doctors now. And I think we should do everything we can to try to shore up that trust and not break it down. And, I'm done.

Paul Egerman – Businessman/Software Entrepreneur

That's a very interesting and helpful comment. And the issue of trust is interesting also when we're talking about a payer panel, where I think some patients might inherently distrust the insurance companies, I don't know, that might be a controversial comment, but –

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

The physicians distrust them, too.

Paul Egerman – Businessman/Software Entrepreneur

I know that and so this issue of transparency could be important as it relates to the payers. One – I'm sorry, and Deven has her hand up. Go ahead Deven.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Well I do, but it's my second round Paul. So, you have – question

Paul Egerman – Businessman/Software Entrepreneur

Do we have anybody else who would like to ask a question? Okay, go ahead Deven

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Paul?

Paul Egerman – Businessman/Software Entrepreneur

Yes, go ahead whoever – was that Wes? I'm not sure.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Paul, this is Wes.

Paul Egerman – Businessman/Software Entrepreneur

Go ahead Wes.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

I just – we have heard a number of providers comment about following up on how diligent they are about following up on patient's privacy issues and I for one don't doubt it in the least. I do think though that we're obligated to look at some mechanism that includes in the balance, situations where that doesn't work. We have to somehow balance off the fact that there are some bad actors and there are some failed processes in organizations with good intentions, as we puzzle through this conflicting set of requirements. Thanks.

Paul Egerman – Businessman/Software Entrepreneur

That's helpful. And I also see that Leslie has her hand up. Leslie?

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Yeah, I'm just sitting here with one empirical wonder, which is, whether anybody has any good data about the actual patient requests that have occurred, or patient attitudes about what they would want to know. I think it might be very interesting if we could actually, despite the fact that there are not a tremendous numbers of the requests that have occurred, if we could actually get information about what patients were looking for with those requests. Because – I mean I actually, since there's a little bit of time here, I'm actually one of the few people who's ever filed such a request. I got met with a it's treatment, payment and healthcare operations and as a result, I have to this day, been unable to figure out which provider revealed my PHI to Utah Medicaid, which then went to Eastern Europe, a security breach.

And what I don't know is, whether requests look like that, whether they look like neighbor requests. What kinds of concerns lie behind patients wanting to know this kind of thing? And I think that might help us figure out where the legitimate mistrust might be and where the appropriate trust might be, too. I'm asking an empirical question and whether there's any way to try to figure that out. I mean I suppose it would be providers that would have the information about the actual requests that they have gotten, however small.

Paul Egerman – Businessman/Software Entrepreneur

That's an interesting comment, I don't know if either of the panelists want to respond.

Scott Morgan, MPH – Executive Director and National Privacy and Security Compliance Officer – Kaiser Foundation Health Plan, Inc.

This is Scott. Yes, I agree much more likely on the provider's side. I think we would need to go do some interviews to actually collect that information, or some kind of survey. I do know that when we get requests, there is – people aren't always clear about the different types of requests that they can make. So, we may log it as is a disclosure accounting request at first, when someone really wants to access their own information. So, however this is looked at would need to take care to kind of distinguish the different needs that people have.

Lynne Thomas Gordon, MBA, RHIA, CAE, FACHE, FAHIMA – Chief Executive Officer – American Health Information Management Association

This is Lynne Thomas Gordon from AHIMA. I have an unusual story. I had been on the provider side for many years before going into association management and this is a little bit of a twist. The last request, although they were very rare to get these types of requests, I was managing large multispecialty and single specialty clinic operations. And we got a call from a patient who wanted to get a copy of who had accessed her record and said that there had been – she had a venereal disease and that it was being spread all over the place and she wanted to know who had released that information. And pretty much named the person she thought had released it. And I was shocked because I knew this was a good employee, but I thought wow, we're going to have to let her go, this doesn't look good, but, we'll investigate it. We did.

It turns out the rest of the story is that the patient knew we had very strict guidelines for confidentiality, security and privacy and that if an employee was found to ever release information like that, they would be fired. Well she was the ex-wife and the employee was the new girlfriend and she was trying to get her fired from her position. So it does show that sometimes patients aren't just trying to – it's very rare and I was very surprised, but it shows you that people know that hospitals take this very, very seriously and in this case, she was really just trying to stir up a hornets nest.

Paul Egerman – Businessman/Software Entrepreneur

That's a very helpful comment Lynne, thank you for that comment. It is actually one of the aspects we've seen from the privacy discussions on other topics that sometimes the issues that I would broadly call family issues, are definitely privacy challenges.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

That's why I think it's really important to try to get non-anecdotal information to see if we could actually get –

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Yeah, but Leslie, I mean I agree with you, but where?

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Yeah, I know. That's why I thought if people kept records of it, it might be interesting to know.

Jutta Williams, CISSP, CISA, CIPP – Director, Corporate Compliance Privacy Office and Chief Privacy Officer – Intermountain Healthcare

Hey Leslie, this is Jutta, and we do keep records and we have kept records. In fact, our database goes back to I think 2002 on all patient complaints that we have logged and investigated and the resolution. It would take some data mining, it would take some effort but we could go back through all of the patient complaints and pull out the trends. And I think that's possible and maybe that's something I can offer to do for the group. Typically, and this is because I am oversight for all of these and so me and my team go through every case, every week. Typically it's family on family, it's coworker on coworker, sometimes it's neighbor snooping. Most of the time, I would say vast majority of the time the intent is good and not malicious in nature. There are those situations where there is malicious intent. There's typically a domestic dispute that's occurring and there's often a child custody issue at hand. Sometimes Department of Family and Children Services, a DCFS concern involved.

But most of the time people do know exactly who it is they're concerned about and/or when they heard something that was inappropriate. But a lot of the time it's not malicious in nature, people are looking if so and so had her baby yet or whether or not it was twins or a single pregnancy. And so we could pull those metrics and statistics out, and we have been collecting them for many, many years. We've seen the numbers drop substantially as we monitor and we respond to incidents and we don't have nearly as many as maybe we did at the beginning. But yeah, we could pull those metrics for you. But that would just be Intermountain, that would just be in our little neck of the woods.

But I do think that it is possible, and I do think that there should be a survey conducted, a true, independent survey that talks about very specific questions about patient interest in this area. Because it's not "us" versus "them," I think that we're thinking we need to balance patient interest with provider burden and so it sounds like "us" versus "them," all we're really trying to do is identify where we should invest our dollars.

John Houston, JD – Vice President – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

This is John Houston, I have to agree completely with that last comment. I think UPMCs experience is incredibly similar to that. So I agree completely.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

If we – Jutta, if you're willing, I think, to take a look at your data and get back to us on this, I – frankly I think it would be helpful.

Jutta Williams, CISSP, CISA, CIPP – Director, Corporate Compliance Privacy Office and Chief Privacy Officer – Intermountain Healthcare

Yeah, it'll take some effort to pull it out because it's all in text fields, it's not like it's readily chunky, but I think that we could do percentages. I'd be happy to do that.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Yeah, we're – we might have more time on this issue than we originally had carved out for ourselves with the potential government shutdown, but we'll talk about that toward the end of the hearing, but that's a very nice offer.

David McCallie, Jr., MD – Vice President, Medical Informatics – Cerner Corporation

Deven, it's –

Jay Schwitzgebel, CISM, CISSP-ISSMP – Director of Information Security and IT Compliance – CareSource

This is Jay at CareSource. I just wanted to add in also that the way others have characterized the nature of the issues that come in, they are very often for CareSource, too, in our experience also the family members and neighbors and those sorts of things. They don't come in the form of information disclosure requests, they come in the form of a complaint that this happened and we spend investigative resources to determine what records we have to prove that that's the case or to defend or confirm. Additionally AHIP has polled its members, has surveyed its members and – results of that survey have been submitted for the record. But they found, in 2013, they have only had 66 privacy complaints this year and across the aggregate 66 million covered lives, that's one complaint in every 1 million covered lives. So CareSource's experiences and that of the broader AHIP organization have been again submitted for the record and that may be useful as well.

Paul Egerman – Businessman/Software Entrepreneur

That's very helpful.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates

– Paul –

Paul Egerman – Businessman/Software Entrepreneur

Go ahead.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates

Yeah, this is Dixie. I think there's – I think we're veering off the topic of keeping and offering an accounting of disclosures –

David McCallie, Jr., MD – Vice President, Medical Informatics – Cerner Corporation

Right.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates

– into how many patients are complaining and I think if we count – I mean, up until HITECH really. I don't think that – and maybe even today, patients have not been aware that they could get an accounting of disclosures of their – and potentially accesses to their health information as well. And I think it's important that we recognize that these are two different things. A patient coming and suspecting something and asking a provider or payer to investigate it is different from making – from a transparency – providing transparency wherein a patient can actually look at the accesses to their record. So I think that a measure of how many people have come and requested an investigation, I would argue is not a good measure of the number of patients who would actually look at a record should it be readily available to them.

Paul Egerman – Businessman/Software Entrepreneur

That's a good comment.

David McCallie, Jr., MD – Vice President, Medical Informatics – Cerner Corporation

This is David, I would like to second that point.

Paul Egerman – Businessman/Software Entrepreneur

Yes, I see you have your hand up, go ahead David.

David McCallie, Jr., MD – Vice President, Medical Informatics – Cerner Corporation

Yeah, I feel like we've drifted into what no one would question are abuses of the system and we all agree obviously that we need mechanisms to remedy those abuses. But I think there's a broader question that we started with, which is perfectly legal uses of the data, but that a consumer would like to have knowledge of what's happening to it, where's that data is going? No one is accusing necessarily that it's an illegal use of the data, but you might want to know which research protocols are using your data, having been de-identified, for example. Or which marketing agencies have been hired by the hospital to have access to your data. And I think that we are drifting into the realm of fires are unlikely, so let's not waste money on Fire Departments, I mean, I don't think that's a – that's really the wrong subject.

John Houston, JD – Vice President – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

But – this is John Houston. I mean, we still have to be practical about all of this. I mean, I think that maybe there's a simpler way. To your point, if you want to know about what ad agencies and whoever else is accessing data, maybe you have some part of a notice or an extended notice, you talk about all your uses of data including what vendors use what type of in – what third parties use what type of information. I mean, we're spending a lot of –

David McCallie, Jr., MD – Vice President, Medical Informatics – Cerner Corporation

And that's – (Indiscernible).

John Houston, JD – Vice President – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

I was going to say, we're spending a lot of money and we're – about something that in practice – the practicality of which is that nobody is asking for. And I just want to be reasonable in trying to meet everybody's ends but understanding that – I agree with everybody else who just said that, we're just not seeing a lot of action here.

David McCallie, Jr., MD – Vice President, Medical Informatics – Cerner Corporation

Well some of that's –

Jay Schwitzgebel, CISM, CISSP-ISSMP – Director of Information Security and IT Compliance – CareSource

This is Jay and if I could com –

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

Paul, this is Walter, could I be added to the queue.

Paul Egerman – Businessman/Software Entrepreneur

Yeah, go ahead Walter.

Walter Suarez, MD, MPH – Director, Health IT Strategy & Policy – Kaiser Permanente

So, yeah, I wanted to jump in because I think there are two different things here we should consider. First of all, I think we should consider thinking outside of the box. We've been trying to frame the entire discussions really around the concept of the accounting of disclosures, and we should step – and accounting of users actually, and we should step back and look at the, what is it that we are trying to achieve ultimately? And see if the best way, the most effective way, the most reasonable way is through an accounting of uses and accounting of disclosures. Or maybe there is an enhanced, improved, more effective way in which consumers can be informed about and pursue investigations and those kinds of things. Because at the end, those are ultimately in many cases, what consumers are interested in when you look at the experiences of organizations that have faced those situations.

So we should really think about this and think about outside of the box and what is it that we are trying to achieve and not try to frame everything around the concept of having to provide an accounting of every single instance for treatment, for payment, for operations. When – the other thing one should consider also is the fact that consumers and providers in a number of cases, most cases are communicating about the disclosures that they are going to make and data that is going to be made – is going to be disclosed. So consumers know they have to disclose the data of the treatment to a pharmacy so that they can go and pick up the pharmacy prescription. Now, I would have to account for use or for that disclosure and then tell the patient, oh yeah, and by the way we disclosed it to the pharmacy, because well, you were prescribed this drug and you needed to pick up it up. So you can imagine the number of instances where the patient would be wondering, why are telling me what you are supposed to be doing and the disclosures that you are supposed to be making in order for me to be treated.

And then lastly I think it's important to consider also the fact that, I think by virtue of attempting to create these mechanisms for tracking all these instances, not only there is a cost associated of course with it, and there is a significant question about the usability of the data back in the consumer end. But I would like to know from a technical perspective what is the degrading factor in terms of the speed of access to data, because now every time someone is going to look at the data, there's going to be metadata attached to it, a lot of metadata, purpose, when, why, how, for what purpose, who is doing this, that. And so every time I open my medical record and see a patient I'm going to be slowed down because behind-the-scenes the system is trying to capture all these pieces of information. So those kinds of elements I think are important to kind of think outside the box and begin to look at alternatives.

Paul Egerman – Businessman/Software Entrepreneur

Those are very – comments Walter, I wanted to make sure I tell everybody, we're still in the question and answer period for our two payer panelists. And I know Deven, you wanted to ask another question and if anybody else has a question for the payers, we should try to do that, but go ahead Deven.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Yeah, I think I just wanted to follow up on the stream of discussion that we had – that I started with on the panel, because I have some follow up questions. And it's the issue of whether in fact the Office of Civil Rights in implementing HITECH, given what Congress was trying to aim at, and there may be a difference of opinion as to what Congress was trying to aim at, but should the requirement look different for different covered entities? What would be the legal justification for doing that, and if that's the case, what would that look like for payers? I mean again, assuming that part of what we're trying to do here is to provide HHS with some recommendations about how to move forward with what Congress put forth in HITECH on this issue.

Dixie Baker, MS, PhD – Senior Partner – Martin, Blanck and Associates

May I comment on that Deven?

Paul Egerman – Businessman/Software Entrepreneur

Well I'd like it if first can we get to the two panelists and see if they could respond to this?

Scott Morgan, MPH – Executive Director and National Privacy and Security Compliance Officer – Kaiser Foundation Health Plan, Inc.

Hi, this is –

Paul Egerman – Businessman/Software Entrepreneur

Go ahead.

Scott Morgan, MPH – Executive Director and National Privacy and Security Compliance Officer – Kaiser Foundation Health Plan, Inc.

I think we're interpreting the congressional intent to be about EHRs only and that, to the earlier comments, there may be times where that includes a payer, but that it really was about electronic health records and we take it for that, not a broader intent for all PHI or all PHI and designated record sets for all covered entities.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Right, but then how would you define the definition of EHR? I mean, there's a definition of EHR and it's not one that says, certified EHR. right?

Scott Morgan, MPH – Executive Director and National Privacy and Security Compliance Officer – Kaiser Foundation Health Plan, Inc.

There are – yes, there are different definitions of EHRs.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

But would you also be comfortable with us coming up with recommendations that would apply to conception of an electronic health record but that has more covered entities in it than just clinicians? And if in fact you think we should have different recommendations for payers say, what would that look like?

Jay Schwitzgebel, CISM, CISSP-ISSMP – Director of Information Security and IT Compliance – CareSource

This is Jay at CareSource. I mean, exactly to your point, I think that it's not a one-size-fits-all. We've heard today the use cases from large providers to small providers to payers are very different. And so as a payer at CareSource, we're using claims systems, I mean, it's a claims system on the back end, it's a payer system that wasn't designed to have this sort of logging. Somebody made the excellent comment that there are performance impacts to turning on the sort of logging that this requires. So when we talk about, what value there'd be in some collection of logs or some sort, and get much more specific than as it's draf – the rule is drafted today, so we can maybe focus on what is useful and what is needed.

Someone commented a moment ago that we were drifting off-topic, and I apologize if that's the perception, but actually all I'm trying to point out is that the only information we have about what the consumer's need is their privacy complaints. So, I didn't think that was off-topic, it's just the best information we have. We don't have any indication the consumer is looking for an accounting of disclosure, they want to know why so-and-so looked at the record and so we want to know if they actually did. The capability internally to a payer is of far more value, I think, than just turning over logs. So, yeah, if we can get to the individual use cases and not look at all covered entities under the same label, maybe we can begin to get more granular about the requirements.

David McCallie, Jr., MD – Vice President, Medical Informatics – Cerner Corporation

This is David, with all due respect, the first panel we heard today represent three separate organizations with large numbers of members who would, in fact, like to have more than just who's just been looking at my record for fear – out of fear of abuse. So, it's not like there's no demand. It's a good question how to balance the demand with cost, I think that's a very valid discussion. But there is demand.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

This is Wes. I just want to make a couple comments. One, the issue is balancing demand with cost and understanding why people ask for information or would ask for information is important in achieving that balance. I think that the statement that payers have claim systems really shorts the possibility of compli – of a need for compliance by payers, because they have care management systems that have data that's very similar to what's in an EHR and that in some cases, are used for decisions that affect whether a given procedure is covered or not. So I think that an examination by our committee of all of the systems and payers with regards to the need for similar protection, would certainly be worth looking at.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck and Associates

May I say something now? This is Dixie. I certainly agree with Wes and I think that going back to Walter, I think the issue that we're trying to achieve here is transparency. And I think if we require an accounting of disclosures and accesses only for certified EHRs and don't have a similar requirement for all of the handling of PHI within payers, we have not achieved the objective, which is transparency.

Paul Egerman – Businessman/Software Entrepreneur

So, again, this is the payer panel and we're just about out of time, but I just wanted to make sure that I thank both of our presenters. We do have one or two minutes if either one of you would like to make any final comments, having heard some of our reactions.

Jay Schwitzgebel, CISM, CISSP-ISSMP – Director of Information Security and IT Compliance – CareSource

This is Jay. I think the only other thing I would add, that I touched on just very briefly in the testimony, is that today the systems that we're using as are designed and available to us from our software vendors don't make this data available. That level of – the degree of logging that would show us when someone views a record in our systems isn't available to us. So when we do investigations to look into whatever complaints we may receive, we're looking at – .at all the data's available to us in a very manual way across all of our systems, including office automation systems, email and things like that to try to determine and recreate an event that may or may not have happened.

The data's just not available to us and in our discussions with our claims systems vendor about what it would take, they describe having to completely dismantle the software and recreate it from about 10% back up, at significant cost. So when we talk about wanting transparency, I can appreciate that. But when we just talk about it like as it's the vision and we don't know what we are striving for, it's difficult I think to people who don't understand the architecture and the infrastructure of these systems and the complexity of how they're integrated. It's difficult to understand what it takes to get there, it's extremely costly and unavailable to us today. That's – point

Paul Egerman – Businessman/Software Entrepreneur

That's a very helpful comment and so I very much appreciate that. And let me thank you both again for participating in our hearing in our panel. We've reached the point in the agenda Deven, where we're supposed to have a brief discussion of next steps and then provide an opportunity for public comment. So do you want to open that discussion, although I think that we've done a little bit of that discussion already.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Yeah, no, we have definitely had a little bit. Thank you very much, Paul. I want to also extend my thanks to our most recent panelists as well as all of those that we've heard from today. And it's been a really very interesting day. So what happens next is the following. We will begin deliberations on what we have heard as a Tiger Team, hopefully on our next call, assuming that it goes as scheduled. Our next call is October 9th, which is a week from Wednesday. However, we need to let everyone know that in the event of a shutdown of the government, if it were to extend to that day, we will not be able to have our call as scheduled, because all of those will be canceled. We'll try not to be insulted that our work is considered to be nonessential, but it's true. Our operations will not occur if, in fact, the government does shutdown.

But assuming that we may be either up and running by then or not shut down at all, we will begin deliberations on this on the ninth. Now we had hoped to be able to take into account not just the written testimony that we received from our panelists as of the hearing today, but also the information on the FACA Blog that I encouraged everyone to respond to. I suspect though, that if there is a shutdown, the ability to post on the blog will be impacted by that as well, which means that you'll just need to sort of monitor things very carefully on the website. Again, under ideal circumstances we would encourage you to get anything in to us in writing that you want us to consider in advance of our meeting on the ninth. However, given the possibility of a shutdown in the government, the timing on that may be disrupted and we'll just do the best we can to be able to process this – our recommendations as soon as possible when we are able to do that.

The other thing I'll note is that we had the advantage of being joined by some of our advisory committee colleagues, so the Standards Committee Privacy and Security working group as well as the Privacy, Confidentiality and Security Group within the NCVHS. We will not be deliberating recommendations together, but each of us considering what we heard today within our respective purviews, but we do have overlap in membership of all three groups and it is our very strong desire to be coordinated so that we're not providing HHS with conflicting recommendations. And the way that we'll coordinate is not by trying to deliberate together, but by using our overlapping membership and conversations among us to make sure that as we pursue our own recommendations, again within our respective purviews, we again, we're not stepping on each other's toes.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

Deven, I wanted to say, this is Leslie, as a member of NCVHS and also the Tiger Team, I very much appreciate the invitation for us to cooperate. And I also think that this is a model of how we can get information in a particularly useful and efficient manner, so thank you very much for the inclusion –

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Thanks for joining us.

Leslie Francis, JD, PhD – University of Utah College of Law – National Committee on Vital and Health Statistics

– and we'll move forward in a decidedly cooperative way.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

So with that, Michelle, I think we're ready to open for public comment.

Public Comment

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

Thanks Deven. Operator, can we please open the lines?

Ashley Griffin – Management Assistant – Altarum Institute

If you are on the phone and would like to make a public comment, please press *1 at this time. If you are listening via your computer speakers, you may dial 1-877-705-2976 and press *1 to be placed in the comment queue. We have one comment.

Michelle Consolazio – Interim Federal Advisory Committee Act Program Lead – Office of the National Coordinator

As a reminder to commenters, it's limited to three minutes.

Ashley Griffin – Management Assistant – Altarum Institute

Adrian Gropper, are you on the line?

Adrian Gropper, MD – Chief Technology Officer - Patient Privacy Rights

I have a short comment and would be happy to take questions in the remainder of the time. I've tried to listen carefully to the great testimony provided today and points for a constructive approach. Automation of accounting of disclosures and related access to the patient information would shift the covered entity's burden of processing logs, educating patients and performing investigations to the patient's agents. Incremental adoption could start with new systems as they're installed and communications with business associates including health information exchanges. Sharing Direct and Blue Button Plus for accounting of disclosures and document exchange would reduce the burden of developing and implementing separate systems and redundant storage. Automation around accounting for disclosures be the first step because it could reduce the burden on the covered entity. Thank you.

Ashley Griffin – Management Assistant – Altarum Institute

Our next comment is from Joy Hardee.

Joy Hardee, RHIA, CHPS, CHRC, CPHQ – Vidant Health Systems

I just wanted to thank all of you, the presenters, OCR, everyone involved today because I think the discussion was just so valuable and I really appreciate it.

Paul Egerman – Businessman/Software Entrepreneur

Well thank you Joy.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Yeah.

Ashley Griffin – Management Assistant – Altarum Institute

Our next comment is from Ginger Fong. Ginger, are you on the line? Moving on to our next comment is from Lisa Scott-Lee.

Lisa Scott-Lee – Sacramento County DHHS/BHS

Thank you very much. This is Dr. Lisa Scott-Lee, Sacramento, California, Department of Health and Human Services, County of Sacramento. We had sent a letter early on in discussion regarding this additional accounting of disclosures and had shared at that time our concern of the continued layering of additional requirements without allowing for the budgeting of such items and the administrative and cost burden that is placed upon us. Would like to reiterate the comments that were made earlier by other providers who had shared this similar perspective. Would also like to reinforce and reiterate that yes, when one has a robust accounting, and tracing back of incidents, we do seem to be the ones who might be highlighted, just because we are so good at reporting ourselves and being so transparent. So, wanted to reiterate that fact that we've noticed that as well, that that might not necessarily be a good indicator of showing we are conducting our due diligence. Thank you very much.

Ashley Griffin – Management Assistant – Altarum Institute

Thank you, Lisa. We have no more public comments.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

So we have booked a lot of time for this, I'm inclined to give folks another minute to dial-in. I was expecting more, I don't want to hold people interminably, because it's been a long day, but I'd like to make sure that there aren't additional comments, about another minute.

Ashley Griffin – Management Assistant – Altarum Institute

We have an additional comment from Marty.

Marty Esquibel – Privacy Officer – Children's Hospital, Colorado

Am I on?

Ashley Griffin – Management Assistant – Altarum Institute

Yes, go ahead.

Marty Esquibel – Privacy Officer – Children's Hospital, Colorado

This is Marty Esquibel, I'm the Privacy Officer at Children's Hospital – Children's Hospital Colorado. And we submitted something online but there are two things. One, we're a pediatric institution and did the rule-makers really consider the impact to treatment and patient care in order to absorb the overhead of tracking external disclosures – let me get back to my comment, for TPO. And this goes to the fact that traditional EMRs, echoing some information security concerns, are not built to easily and quickly track everyday disclosures that come from the clinical level. And we have – that where we, as in a hospital interact with numerous practices, schools and other organizations and these are daily disclosures going back and forth, and there is not a clean mechanism to just cover that administrative burden. And we're talking about hundreds of disclosures per day. And that's it.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Thank you. Okay, is there anybody else?

Ashley Griffin – Management Assistant – Altarum Institute

We have no further public comments at this time.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Yes, this is Deborah Peel.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

I think the day –

Paul Egerman – Businessman/Software Entrepreneur

I heard Deborah Peel trying to say something.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Oh, I'm sorry.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Sorry, I've been trying to call in. Yes, I just –

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Deborah, we can't hear you very well.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Is this better?

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Yes.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Sorry. So sorry. I just wanted to offer myself and also Adrian Gropper, our Chief Technology Officer as resources to many of the people that spoke today. There seems to be a lot of people that don't really understand that there's a great body of work including studies, letters and all kinds of materials about what the public actually really does think. And in our comments today that we submitted formally, we put in a history of how the accounting of disclosures came about, that you all would find interesting. The reason really was for transparency and accountability, because we have no control over our data. It wasn't about specifically investigating breaches, although of course that's wonderful and should happen.

But we're in a position, all of us, of not knowing where our data flows. And so, on our website, and I think I put some materials in our remarks as well, we do not even have a data map of where all the data flows. And I know all of your institutions care about patients and are doing the best you can, but we've got to look at the fact the data doesn't stay where anyone thinks it does. And we don't even have a complete map. We're working on that with Professor Sweeney at Harvard. Anyway, so we'd like to offer ourselves as resources if we can help you in any way with any more specific information about patients. But also every year we have an annual international summit on the future of health privacy. The last one was in June, in Washington, it's always at Georgetown Law Center. And we had Peter Hustinx, the European data protection supervisor as the keynote, along with Todd Park, Leon Rodriguez, Mark Rotenberg and even Justice Brandeis' biographer, Mel Urofsky.

We had some amazing people speaking and we always have plenty of patient advocates and privacy experts there too, which I think unfortunately people in industry just don't have many chances to meet. And the summit, the summit is free and it's handy and it's the first week of June in 2014. So, please let us know if you're interested and if we can help you, because we would really like to.

Paul Egerman – Businessman/Software Entrepreneur

Terrific, thank you very much, Deborah.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

You're welcome.

Paul Egerman – Businessman/Software Entrepreneur

Thank you very much Dr. Peel, sorry.

Deborah C. Peel, MD – Founder – Patient Privacy Rights

Oh, Deborah's fine. Don't be silly.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Okay. So thanks to all for hanging in for a long but extremely productive day. And hopefully we'll be able to get to deliberating these issues very soon. Thanks Paul.

Paul Egerman – Businessman/Software Entrepreneur

Thank you Deven and again, thanks to everybody. Take care, bye, bye.

Deven McGraw, JD, MPH – Director – Center for Democracy & Technology

Bye.