ORPP&E Webinar
Date: March 24, 2021
Session: Enterprise Research Data Security Plan (ERDSP) Role-Based Training for Principal Investigators/Institutional Review Board (IRB)/Research & Development (R&D) Committee Stakeholders
Presenter: Terry Peters, Carol Johnson, DuJuan Williams

This is an unedited transcript of this session. As such, it may contain omissions or errors due to sound quality or misinterpretation. For clarification or verification of any points in the transcript, please refer to the audio version posted at
http://www.research.va.gov/programs/orppe/education/webinars/archives.cfm

Terry Peters: Yeah, just bear with us for a second. The slides should be coming up here in just a second. Now someone just put in the chat they were having a hard time hearing my voice. Is that a little bit better?

Moderator: Terry, it might be that user. I can hear you totally fine.

Terry Peters: Okay. Great. Thank you. Okay, Carol. Yeah, now I can see it. Great, thank you. Okay, again. You know my name is Terry Peters, with the Research Support Division. And we're going to have a training session today on the Enterprise Research Data Security Plan for research investigators and staff. As well as other R&D stakeholders that have a stake in the ERDSP plan. Next slide please.

Next slide please. That was one we had for our other sessions when we used Teams. Okay. For the agenda today we're going to cover several items. One of which of course is the importance of the ERDSP toolset. We're going to discuss the roles and responsibilities as it pertains to the ERDSP. We have a little overview of the ERDSP process when it you know when the protocol review process, where it fits in. We're also going to review the phased implementation schedule of the ERDSP. As well as, you know provide guidance on when a protocol requires an ISSO review. Right? With the ERDSP, the ISSOs will not be required to review all research studies and amendments. They'll only be reviewing the ones that are high-risk. We'll also review the use of the ERDSP toolset. We have several training scenarios that are embedded in the slides. We'll walk through those. And then in the end, we're going to give you a little demo of the ERDSP. We're actually going to bring it up, and we're going to fill out the first three sections. Just to show you how it works. And then we're going to walk through submitting the ERDSP toolset feedback. We do have a site set up so that you know if there's issues or recommendations for improvement or anything. We greatly appreciate any input that you can provide. Next slide please.

So why is the ERDSP necessary? Well you know it was developed in accordance with the recent amended technical policy amendment to VHA Directive 1200.01. It is an Enterprise, standardized template and data security plan that's designed to provide research principle

investigators with a tool to aid in documenting the safeguards to protect research data information and resources. It also provides the PIs a mechanism to document their plan for managing risk to protect research data with a research protocol. And it also promotes the standardization of the ISSO review. Because you know we have received a lot of feedback from the field about how the ISSO reviews are not standardized across the board. And this is our first step in standardizing those reviews. It also assists the Principle Investigator in documenting how that research data will be used and protected throughout the research protocol's lifecycle. And again you know part of the development of the ERDSP was in response to, we did a RSD in collaboration with ORO, ORPP&E, as well as I'm sorry ORD, ORPP&E, as well as the Office of Research Oversight risk program. The comprehensive risk assessment on research protocol of data management as well as also using in that risk assessment the 2018 ORD, ORO research information security vulnerabilities memorandum. Which outlines several systemic vulnerabilities that is seen kind of across the board. And so you know the risk assessment along with that memorandum, you know assisted in the development of the ERDSP. Next slide please.

So again, why is it necessary to introduce a standardized process for conducting the ISSO research protocol review to support effective research protocol of data management. One thing we did here for that bullet right there is in the ERDSP guide at the end of each section that we're going to cover today, in the guide we have provided the ISSOs a list of things that they need to check so that we standardize that process right? Standardize the ISSO review process. The ERDSP also improves the data security planning processes for research protocols by PIs and research data stewards. It also enables the ISSOs to more consistently review and assess risk associated with the protocol and the study. And the toolset includes a tailored baseline of information security controls that maps to critical administrative, physical, and technical security controls to the NIST Cybersecurity Framework. Next slide please.

So we're going to touch on some of the key stakeholder roles and responsibilities. Just for time today. Because you know once we get into the different questions we may have to spend a little time on those. We're basically going to touch on the roles and responsibilities of the Principal Investigators and the local facility ISSOs. Your Principal Investigators are responsible for completing and submitting an ERD for each proposed and or amended research protocol. The PIs are also responsible for coordinating and collaborating with the ISSO to resolve research study related information security compliance issues. And just as an FYI this is something that on our training session with the ISSOs, we have encouraged them you know to, when there's an issue with a research protocol you know to meet with the PI. Right? Versus you know emailing back and forth. And you know meet face to face or over a Team session and kind of you know get those issues resolved. Right? Because you know we understand that with these protocols there's time constraints. Right? And you've got to get that in by a certain time, the IRB, we want you to meet those deadlines. With the local facility ISSO, they're responsible to provide guidance to Principal Investigators and R&D Committee stakeholders in resolving research information security compliance issues. They also review high risk research protocols that are identified within the ERDSP toolset. And again, you know the ISSO is only going to review research studies that are considered high risk. And we're going to walk through how that's done. It's actually a pretty simple process. Next slide please.

This is just, these next two slides are just kind of an overview of that process. You know where you know the PI does complete the ERDSP. They then, when completing the ERDSP they determine if the research study is a high risk study. If any of those research study conditions apply. And we're going to talk about that here in a minute. That will be a lot clearer to you in a minute. And of course, if those high risk conditions apply, that research study does get submitted to the ISSO for their review. As well as if you have a research study amendment that amends any of those high risk sections or questions in the ERDSP, those also require review. If there are no research study conditions apply, or there is no change, the high risk sections of a research study amendment, then of course, one, the ISSO does not review those. But also on the form there's only like one question and a signature that has to be done. So it's pretty straightforward. Next slide please.

When the ISSO of course receives it, the ERDSP along with that protocol submission package. They review the ERDSP as well as the research protocol to determine if the ERDSP is adequate and compliant. So while you know when the ISSO gets that document, right, they're going to not just review the ERDSP, they're going to review it, but they're also going to review you know the rest of the documents in that submission package to validate that the ERDSP is correct. If there are any corrections to be made of course they will return it back to the PI for those corrections. Once those corrections are made, the local ISSO signs off on it that it's compliant with the VA security policy. And of course, in this whole process if there are any issues or things that can't be resolved or guidance as needed, the local ISSO can also reach out to us, because we're here to assist. And then the PI submits the approved ERDSP with the protocol to the R&D Committee, or subcommittee. Next slide please.

So we mentioned at the beginning there that you know we're doing a phased implementation. So the ERDSP is required by technical amendment 1 to VHA Directive 1200.01. So what we're doing from March 22nd to April 19th we're conducting a pilot and soft launch with 30 VA research facilities who will begin using the toolset during that time period. And we do have the list of sites on the next slide. Now in phase two, which is April 19th to April 26, we're going to collect feedback from those sites, we're going to make any changes that are necessary to the ERDSP toolset, or to the guide. And then we're going to come back, and you know for those sites that were not part of that pilot, soft launch, we will again provide training to the field between April 26 and May the 7th. We will have you know some firm dates here soon on that. And Phase 4, which is May 10th, the ERDSP will be required for all research studies and amendments that are submitted to the R&D Committee. Now real quick, I just want to say this real quick, for the sites that that are not part of the pilot and soft launch, you are not required to use the ERDSP. It is recommended you just keep using your current processes until we go fully operational on May 10th. Next slide please.

These are the sites that are part of the phase implementation plan. The 30 pilot and soft launch sites. These are also in the slides that have been sent to everyone. So you'll have a list of those sites. Next slide please.

So when is the ERDSP required? We kind of touched on it, we want to just kind of do it one more time. For new research protocols, and the ERDSP's required for all new research protocols, you know human, animal, and basic laboratory. Now the reason we have new next to that is, you know when the ERDSP is implemented at your site, there is no reason to go back for previous protocols and do one. Right? So it's going to be for new. For a research study amendment, and the ERDSP is required to be completed for all research protocol amendments. Now there is a little caveat in that, but we will get to that towards the end of the training when we start talking about amendments. Next slide please.

You know we were talking about earlier about the ISSO only reviews the ERDSP if it's a high risk study. You know the high risk conditions, right? So what are those conditions? And these are, these will appear when the PI is completing the ERDSP template. There are four of them. And we will get a little deeper into these as we start going through the questions. So I'm just going to lightly touch on them here. Will any VA Sensitive Information be accessed, stored, generated, or transmitted during the research study? That's one of the conditions, right? If that's marked yes, then an ISSO review is required. Now I do want to point out that it's kind of a little bit of a—we have seen with DoD and several universities that do a lot of research, that this question here is what triggers their ISSO reviews as well. The second one is, will the research study use any VA mobile devices or mobile applications? The third one is, will any research study protocol data be transmitted or transferred to an external entity? And will the research study use any external information systems or devices? Now I know that some people may think that the third question and fourth question are similar—and they are. But there is a slight difference in it, in that in the first one we're talking about transmitting data or transferring it. Right? We're not talking about using a system, but you know basically sending the data out, right? The fourth part is about you know are we using the external information systems or devices in the study. Now to point out real quick, you know the third one we have, will data be transmitted or transferred, what's the difference? Right? Transmitted is when you transmit it electronically. Transferred is when you use a CD or DVD to disclose that data, or a thumb drive, or an external hard disk drive. That's when it's transferred. But we'll get more into these when we get down into the sections. Next slide please.

This slide here is just to address, you know when the, so we have studies that the ISSO will not be reviewing, right? Where all those, where those four conditions are marked no. So how do we know if the ERDSP was completed properly if the ISSO did not review that? We are currently working with Enterprise Security Operations which is who the ISSOs fall underneath, to develop a process for auditing research studies and amendments not requiring an ISSO review. The audit process will be incorporated into the Enterprise Security Operations Research Information Security Compliance SOP and the SOP will also be updated to align with the technical amendments in VHA Directive, 1200.01. Next slide please.

So of course you know before we can start completing the ERDSP we need to know where it's at. We do have it in a couple of different locations. We're going to touch on those real quick. And at the end of this briefing, we're actually going to navigate to those and show you where they are. So for, you know for facilities that have transitioned to the VAIRRS application, the

template can be found within these following libraries under forms and templates. You'll see the VAIRRS library, it's a little dropdown there. And these four here have the ERDSP toolset as well as the guide. And any time you go to these libraries that will be the most up to date version of the ERDSP toolset and guide. Next slide please.

What if we're not using the VAIRRS application? For those facilities that have not transitioned, both the ERDSP and user guide are available in the research, in the ORD toolkit for Research Information Security and Cybersecurity. And it is also available on the Research Support Division SharePoint. And both of those have links right there to that. One thing I do want to point out, you know because the ERDSP is new and it does sometimes you know ask some in-depth questions, it's highly recommended that when a PI is completing the ERDSP template, right? To use the guide you know side by side. Because the guide lays out for you what we're looking for in the response to that question. Right? We have a lot of information there that will help you to answer that question properly. So we highly recommend you use the guide with that. Because you know one of the things is the goal of this ERDSP, one of the goals, or several, but you know one of them is we want you to be able to, for the PI to complete that ERDSP, to send it in. The document has all the information that the ISSO needs. They can quickly get that review done and then you know the study is on its way to getting approved, right? We don't want studies being sent back for additional information. We want to streamline this process and get this research study started. Next slide please.

In the ERDSP toolset we have several sections. You know nine of them to be honest. The first section we're going to talk about, those research study conditions. Section two is data classification. Section three is data sources and collection. Four is data access and storage. Section five is data sharing with VA research facilities. Section six, a little bit long here, we're probably going to cut that one down, that's VA mobile devices and media, as well as mobile apps, medical devices and research scientific computing devices. Section seven is VA software. Section eight is agreements, authorizations and contracts. And section nine is data sharing with external entities and external information systems. Next slide please.

Okay. So once you've started that ERDSP, right, you're going to come down to section one which is the research study conditions. One thing before we start here, I want to point out something, this template, or toolset, is a branching logic form. So when you look at the form initially you're not going to see any questions on it until you do the dropdown box that says this is a new protocol or this is an amendment, right? Then what it does, it generates one question. You answer that question, then that starts opening up new questions, right? So the good thing about this is, while this may seem long when we go through this today, you are probably, it's going to be rare for anyone to have to answer every question. You know in most cases a lot of them won't be presented to you. And so you know it won't be as long as it's going to look today. So in section one, we had the research study conditions for the PI to respond to. I think number one is pretty straightforward, you know will any VA system information basically used in the study, right? Be accessed, stored, generated, or transmitted during the study? The second one is, will the research study use any VA mobile devices or mobile applications? One thing I want to point out on this you know this is one of those systemic vulnerabilities that were

identified. In that there was a lot of mobile devices that were being used that were not on the VA approved list and they were not accounted for on a VA EIL. And in some cases they were not encrypted. The same goes for mobile applications. A lot of mobile, not a lot, but some mobile apps were being used that were not submitted to the appropriate section to be you know reviewed and approved for use in the VA. Will any research study data be transmitted or transferred to an external entity? That one there, you know we have had cases where that data was being transmitted with sensitive data and it was not encrypted in transmission. And so we do have a process as well to help out with that. And then, will the research study use any external information systems or devices? The key here with the external information system or devices, you know in most cases—there are some exceptions of course—that you know an external information system or device cannot be used to collect, process, or store VA owned data unless that system has an ATO, a VA ATO or there's a data use agreement or an MOU in place. Next slide please.

So let's just touch on, I think we got two training scenarios here for the slides. Just to kind of, for the condition of this, just kind of touch on those real quick. The Tampa VA is participating in a collaborative research study with the University of South Florida. Each VA research subject has executed a HIPAA authorization for the disclosure of a copy of their data to the University of South Florida. The VA will disclose a copy of the de-identified research data to the collaborator using an encrypted CD/DVD. How should this question be answered? Of course, it should be answered yes, VA research data is being transferred to the University of Florida using an encrypted CD, DVD. Next slide please.

And this is for the study condition four, about external information for devices. The Atlanta VA will be conducting a VA only TBI study. The study plans to use a research scientific computing device owned by their affiliate university. And the device is connected to the affiliate university LAN extension located within the Atlanta VAMC. How should this question be answered? It should be answered yes, because the research scientific computing device that belongs to the affiliate is considered an external information system. Next slide please.

Okay. Now we get into section two. One thing that we have for section two as well as in the guide we have a data classification table for the different types of VA research data, and we categorize them here. Either sensitive or non-sensitive. Just real quick, this was a collaborative effort between the Research Support Division, the Office of Research and Development, ORPP&E, as well as ORO Research Information, the risk program excuse me. So let's start off real quick with sensitive data types. Of course Individual Identifiable Information, PII, PHI, and then in animal research, the you know Category D and E with picture and video are also considered sensitive. Human genomic as well as Intellectual Property. So what are our non-sensitive data types? First, de-identified research; unpublished research which includes basic animal except for category D and E with picture and video; non-human and basic lab. Animal research category B and C are also considered non-sensitive types. Now the reason we have the public data types broken out on the right here, they are considered non-sensitive. The reason they're broken out is when the risk assessment was done, you know it gets assigned a baseline impact of high, moderate, or low. And so for public data it was categorized as low. And that's

why we have it broken out. But public data types include published research, right? So that's also a non-sensitive data type. Just down below here you can see the policy references that were used in determining these sensitive data types. Next slide please.

Yeah, I think this one is probably pretty straightforward. The North Florida, South Georgia Veteran's Health System will be conducting a collaborative animal research study with their affiliate university. The research study data collected will contain picture and video of mice assigned to USDA Pain & Distress Category D and E. The VA will be electronically sharing a copy of the study data with the affiliate university. Should the data be encrypted in transmission? And yes it should be; again category D and E with picture and video is considered sensitive. Next slide please.

Now we're going to get into section three. Data sources and collection, right? And this is where the PI is going to go through and identify the different data sources that are being used as well as those collection methods. One of the first questions is, you know does the research study involve more than one participating site? Now this is a yes or no question. And just to clarify, and this is also in the guide, when we talk about you know more than one VA participating site, we're talking about VA sites that are listed in that protocol submission package, right? So it's just those sites that are in this submission package. So if you have more than one site, you will click yes. And that will bring up the next question which is, provide the name of each participating site listed within the IRB application. Number three is, select the data sources to be used in the research study. And select all that apply. Right now the available selections that we do have on the template are listed right here. We do have others as well. So if your source is not listed you can check other and then that will on the next slide we'll see where that presents you a place to list that other data source that's going to be used. Next slide please.

And question four would popup. Describe the other and or database sources used in the research study. On the previous slide, one of the selections also, databases. Of course you would identify what other source is, as well as you know the database, right? What's the name of the database. Where is it located? Et cetera. Question five is select the data collection methods that will be used in the research study. Again, we have a set of available selections here. We also have other if there are some that are not listed. And what we've done with this template for the sources and the collection methods, we put in here the most common ones that we see when we're doing reviews of research studies. So as time goes on we may expand this list to make it easier on, you know the PI, to fill it out to just try to have the ones that are most commonly used available. And they can just check it off and then yeah, move on. If other is selected, then question six will appear. And will ask to describe the other data collection methods used in the research study. Question seven is, will the research study use any VA applications or websites? Now we're talking like REDCap, VINCI, those kind of things. If that is answered yes, then you just provide in that box that pops up the name and the web address of the application or websites that will be used in the research study. Next slide please.

Okay. In this training scenario, the San Antonio and Houston VAs were participating in a VA only multi-site study. The study plans to use the University of Minnesota REDCap application to

collect study data from each participating VA site. Does the University of Minnesota REDCap application need to be evaluated for a VA ATO? And the answer is, yes. Because in this scenario it's a VA only study, and you have two VAs. So the University of Minnesota is not a collaborator on the study, but is acting as a third party and collecting data on behalf of the VA. The University of Minnesota REDCap application will need to be submitted for an ATO determination. And of course, we're talking of ATO determinations also. You know we cover that in the guide pretty in-depth, so. Sorry, Carol, next slide please.

Section four, data access and storage. And the first question here is, and this is a question for the PI, right? Is will access to the research study's electronic data employ the concept of least privilege, allowing only authorized accesses to users which are necessary to accomplish assigned tasks in accordance with VA organizational mission and business functions? And so what, this question is more to affirm to the PI, right, that we need to employ the principle of least privilege. You know with our electronic data. With our paper data. What, now I think this is also one of the systemic vulnerabilities is that a lot of times you know data that's stored on the VA network in folders, those folders aren't restricted to individuals with a need to know. Right? To the PI or to the PI and the study team right? Sometimes they will have a lot of people that have access to that file, or that folder, that have nothing to do with the study, right? So we have got to make sure that we limit access to our electronic data, as well as our hard copy data, to individuals with a need to know. The next question will be, describe how sensitive hard copy, paper documents will be physically secured. Now in the guide, we provide several examples of this. And a good example is, you know the PI is going to store it in their office, and access to the key is limited to the PI, or the access to the key is limited to the PI and the study team. Right? A lot of times people will say that you know the data will be stored let's say in the PI's office. But they don't talk about you know how is access to that key limited right? So for least privilege we've got to you know limit it to individuals with a need to know. Number three is, provide the storage location of VA research study electronic and paper data stored at the VA or offsite locations. Now, when we're talking about the storage location of your electronic data we need the file path to where that data is located. We frequently see studies where it will say, you know it's on the S drive in the research folder, et cetera. Right? You know with the S drive or the T drive, those numbers are very subjective. And the reason we need the whole file path is unlike years ago where when you say your research data, right? It was at your local facility, there's you know, it's a handful of servers, right? So we kind of all know where it's located at. But now, you know a lot of our personal drives, our email, a lot of things are in the Cloud. Right? So we need to know, we need that file path so that we know where that data is located. Now if you are uncertain of where to, you know how to get that file path, right? You know you're not an IT person et cetera. You can submit a YourIT ticket to your local IT staff and they can assist you with determining what that file path is. Now when it comes to paper data stored at the VA, or offsite locations, and for this question here, we need the location as well as the building number and the room number where it's located. The reason we need the location is, you know a lot of sites have multiple facilities. And so we just need to know you know which one that it's stored in. Number four, will the research study use a standalone computer, medical, or research scientific computing device? This is a yes or no question. If it's answered yes, that will take you to question five. Which asks you to describe the process to back up the

VA research study data stored on the standalone computer systems, medical device, or research scientific computing device. So you know there should be a plan in place. Right? We can't, if we left it all this data that we collect during the study on that standalone computer, or a medical device, or a research scientific computing device, if there was a hard disk failure or something then that data is gone, right? So there needs to be a plan in place to back this data up. So that these devices don't contain the only copy of that data. Next slide please.

And we kind of touched on this one already I think. But you know Dr. Williams is preparing the ERDSP for his new research study. And the ERDSP requires Dr. Williams to provide the storage location—the file path—for electronic data stored on the VA network. How can Dr. Williams determine the correct file path to the data? And we've had some sites that you know they reach out to their administrative officer who can assist with that. If that is not an option, then of course as we just mentioned, submit a YourIT ticket to the local ITOPS and User Operation staff requesting assistance in determining the file path to the data. Next slide please.

Now we're getting into section five, which is data sharing with VA research facilities. Which are, with our first question on this, is will the study share data with another VA facility? This is a yes or no question. If it's answered yes then the next question will appear which is, provide the name of each VA research facility that data will be shared with and describe the method used to securely transfer the data. This is one of the things that will really help your protocol get to the ISSO the first time. Right? Generally in research studies in the past, you know the protocol as well as the submission documentation that goes with that outlines you know who data is being shared with. You know? Generally that's listed in the ICF and the HIPAA right? But what it doesn't tell you is what's the method used to securely transfer that data. Right? Because if that data is sensitive it needs to be encrypted in transmission, right? Now one thing that we have done in the ERDSP guide, we have a list in there of every, different ways that you can transfer data to other VA research facilities. You know whether it's a shared folder that's accessed and being read by both facilities. Whether it's a CD, a thumb drive, an external hard drive, using VA email. Right? But we have a whole list of those in there and we actually outline the security requirements for using those for you. Number three is, will research study personnel physically transport sensitive data outside their facility? Yes or no question. If it is answered yes, then question four will appear. And it will ask you to describe how the sensitive data being physically transported will be secured during transit. Now in the guide we do provide some examples of that. You know like using a locked container, you know a locked briefcase, you know something that you can, you know that kind of secures in your vehicle while you're transporting it. And we have had a case, I mean I've experienced myself, where we had a PI, or a member of the study team that was coming from one hospital to the other. They were in a car wreck, and the data was not recovered. Right? However, we had an authority to transport on file for them. So when it came time, we had to submit an incident ticket. Right? To the CSOC to say hey, you know we lost this data. And of course, one of the first things they ask is you know is it sensitive. Right? How many Veterans were affected? Because we had that authority to transport memorandum, we were able to quickly answer those questions. Right? You'll get a lot of attention when you put in a CSOC ticket for lost research data. And when they ask you if it's sensitive or not, if you say I don't know right? That gets a lot of unwanted attention. Right? So but by having these

authority to transports, right, it really allows the facility to know what data is being transported outside the facility. As well as the sensitivity of that data. Next slide please.

The Portland VAMC is participating in a COVID-19 research study that requires VA research staff to collect nasal swabs from VA research subjects' homes. Study staff will be using a laptop during the visit to collect sensitive information from the research subject. Are study staff conducting the home visits required to have a documented authorization to transport sensitive information outside the VA controlled environment? And the answer to that is yes. I think this is, in the VA I don't necessarily think that people are kinda clear on this, that's why I want to clear it up now. In that if the sensitive information is being transported, right? It requires authority to transport. It doesn't matter if it's in paper format or if it's in digital format, like on an encrypted laptop, you still need to have one. Right? Now in the guide we do provide guidance on this, you know where to look for the guidance as well. I will note one thing, the ISSO is not involved in this process. They were removed from it several years ago. But we do provide some guidance in there for where to look for completing this document.

Okay section six. Which is VA mobile devices, media, mobile applications, medical and research scientific computing devices. So for this section when it first starts out, and what it asks you is, if a VA mobile device, media, mobile application, medical or research scientific computing device will be used in a research study, select the appropriate box. The reason it does this, let's say you did not, you had some mobile devices, but you don't have any VA mobile applications, right? So by checking the mobile device box you're only going to see those questions and not the mobile app questions, right? And this is why we have this one question kind of breaking it out. Now you can select both of course. And then that will present you with all the questions. When you do, do that let's say you're having you know both of these types in there, it will then present you with the VA mobile device media and medical and research scientific computing devices section. Which is separate from the mobile apps. The first question is, is select the type of VA mobile device, media, portable storage, medical or research scientific computing devices that will be used in the research study. And then of course you have all your selections there. I do want to clarify something, you know when I say select the type of VA mobile device/media, so an audio recorder is a mobile device. Mobile media is a CD or DVD. That's why we have them both like that. Right? Because one's a device and one is media. Next slide please.

When you are using you know VA mobile devices, or medical or research scientific computing devices in the study, the question two asks you to provide the make and model, as well as the EE number for each mobile, medical and research scientific computing device that will be used. Now we're talking, you know in this section we're talking VA. Right? Now this is another systemic vulnerability that was noted over the years in that you know a lot of computers, mobile devices, scientific computing devices, are not listed in a VA equipment inventory list and thus they do not have an EE number assigned to them. Right? So all these devices must have the EE number on them. Number three, are all VA mobile devices and media and portable storage devices encrypted with FIPS 140-2 or successor validated encryption? In the guide we do provide a link where you can go and look up those portal storage devices to see if yours is encrypted. However, you know if OI&T has issued you a mobile device or portable storage

device, you can go ahead and answer this question yes. Because they verify that what they're issuing out is encrypted with a FIPS 140-2. Number four, will VA mobile and portable storage devices that contain the only copy of VA data, be backed up at regular intervals? Again, this is kind of like the other section where if you've got a mobile or a portable storage device that has the only copy of that VA research data, then that data needs to be backed up at regular intervals, right? So there needs to be a process in place, which kind of ties into question five, you know describe that process for backing up that mobile and portable storage device. Now, this is the second time we've talked about backing up data on one with standalone devices now we're in the VA mobile and portable storage devices. You know if you don't know how to back up that system right? You don't really know how you're going to get that data from that standalone device, or that mobile or portable storage device on the VA network. In the guide we have, you can submit a YourIT ticket to your local IT staff, and they can assist you in developing a process to move that data off those devices. Number six describe the process for securing VA mobile and portable storage devices when not in use. Again, you know the requirement is for these devices when you're not using them it's the same as your paper documents, right? They need to be, you know, secured when not in use and access of course to those devices needs to be limited you know with the individuals with the need to know right? So. Next slide please.

VA mobile applications. Will the research study use any VA mobile applications? It's a yes or no question. If the answer is yes then question two asks for the name of that mobile device, mobile application, the application owner, and the download link to access that application and the purpose of the application in the research study. Number three asks, has the mobile application been approved for use in the VA? Now if you're going to, you've got a new research study that's coming up and you want to use a mobile device that's not approved—I'm sorry mobile application, I've got mobile device on the brain today. Mobile application that's not been approved for use in the VA we lay this out for you in the guide. So if the application has already been developed there's a process for that through the mobile device management team. But let's say you want to develop a mobile application for your study, so you're just kind of in the planning stage and you're kind of talking about it. Then in the guide we lay out another, you know for developmental, when you're developing a mobile app there's a process for that that uses a VIPR request. And I want to really key in on that, if you want to develop a mobile app, it is really critical that you follow that process before you really get into it. Because there's a team there that will help you. They will guide you through this process and assist you where necessary, right? Versus kind of going through it on your own because you don't want to develop an app that won't meet VA security requirements right? So working with that team, that works those mobile apps will help you a lot. And we do have that process outlined in the guide how to do that. And just real quick you know, we've tried to outline in the guide pretty much any of the situations you come up in, right? I mean including you know if you've got a mobile, let's say you've got a voice recorder and you want to connect that voice recorder to your PC to download the data right? Well in the guide we tell you how to do that. So in this guide we've really tried to capture all the things that will help you get your research study up and running and get it approved. Next slide please.

Okay. In this scenario the Boston VA is participating in a collaborative research study with their affiliate university. Each research subject has executed a HIPAA authorization for the disclosure of a copy of their study data to the affiliate. The VA PI plans to purchase an external hard disk drive with grant funds to transfer the data to the affiliate university. What steps should the VA investigator take before purchasing the external hard disk drive? The first step that a PI should take is consult with their local Area Manager and obtain their approval to purchase that external hard disk drive. Okay. Again you know the area manager is the person that's going to, you're going to need to connect it to the network, right? And so you need to coordinate with them first thing and get them onboard approving that. Otherwise you may buy an extra hard disk drive and they won't allow you to connect to the VA network. Once the area manger concurs, then you want to verify that the hard disk drive being purchased is on the security engineering list of approved FIPS 140-2 Validated Removable Storage Devices. There's a list of approved devices out there. Now let's say the one you want to buy is not on that list. There's also a process, and we outline in the guide, to how you can submit that hard disk drive for review and approval for use in the VA. Again, if you're going to do that, if you're going to submit it, all you do is you submit the make and model, et cetera, and then they will, they have a process to review that. You don't want to purchase it first, right? You want to get their buy-in, get it on the list, and then purchase it. After purchasing that external hard disk drive, the device must be added to the appropriate VA EIL. And an EE number will be assigned to it. And again, in the end, the device must be securely stored when not in use. And I just want to touch on one thing on this slide, Carol, just one second on that last one there, yeah, now this process that we've laid out here, this is a process that has worked at a lot of sites, but there's no official process for purchasing you know IT equipment using grant funds. Now the research information security task force has several sub-working groups that are working on a lot of these you know research IT issues. And one of them is, and it's one that actually I'm on as well, to develop a process where you can use grant funds to go out you know and buy IT equipment that you need that OI&T cannot supply. So we're actually working on that to get a process laid out, right? And then get it put into the correct handbook or directive so that that process is standardized across the board. Because you know I mean we understand in RSD that a lot of times OI&T does not have the equipment you need. I mean you may need a hard disk drive that you know let's say 20 GIG. And the local site only has ones that are 3 GIG right? So it really doesn't work for you. So we totally understand that. And that is being worked through and we hope to have a draft of our recommendation report to resolve that some time this summer, we're hoping. Next slide please.

VA software, this is a pretty straightforward section. It only asks three questions. Will any software be purchased or acquired for use in the research study? That's a yes or no question. And again, you know if you've already got this software installed on VA computers, you know you don't need to list it. This is only for software that you're going to purchase or require for use in the research study. If you are going to purchase some software one of the first things you need to make sure before you purchase it, is the software approved for use in the VA Technical Reference Model? In the guide we do provide you a link that you can go to the list of approved software. And you can see if that software is approved. And question three, provide the name of the software, the vendor, the vendor website address, and the purpose of the software in

the research study. All those are pretty straightforward. You know but back on question two there, you know we do provide you guidance on seeing if it's on the approved list. And then if it's not we also provide guidance on how to submit that software to get it approved by the technical reference model. Next slide please.

This training scenario actually looks pretty similar to the one you previously saw. But it's for software. A VA PI plans to purchase research analytical software for use in a research study and the software will be installed on a network connected VA computer. What are the steps the investigator should take before purchasing that software? Again, you know coordinate with the area manager. You know get their buy-in on purchasing that software. The PI will then need to verify the software is listed, the TRM, Technology Standard List. The PI should also review the decision tab of the software's TRM entry in the TRM Technology Standard List to ensure the version of the software being purchased is approved for use, and the planned usage of the software meets the decision constraints. Now that was kind of a mouthful, right? Basically what you do when you go to that TRM Technology Standard List, you go to that list and you'll see okay, yep, there's my software right there. It's approved in the VA. Then what you do, is you go and look at the decision constraints on that software. It's a tab that's on that software approval right there. It will list the version of the software that's approved. Right? You know there may be only one version of that software approved in the VA. And it may not be the most recent one, right? So you want to make sure that what you're buying is an approved version. Then you want to look at the decision constraints. Because depending on the vulnerabilities with that software, the use of it in the VA may be quite limited. Right? They may limit it only to certain devices or in certain circumstances. Or they may limit it only to non-sensitive data. So you want to review those decision constraints to make sure that they're not going to interfere with what you want to use this software for in this study. And then again, you know if the software being purchased is not on that technology standard list, it must be assessed by TRM before it's purchased. And of course, we have a link right here as well as in the guide where you can go in and submit that software to have it assessed. And one thing else I wanted to touch on this right here, I don't think a lot of people may know this, but you know we're talking about the technical reference model, right? That's your list of approved software in the VA. Now TRM will only approve software in most cases if it is going on a network connected computer. If it's not on a network connected computer, in most cases it is not required to be submitted to TRM. Within the guide we do provide you a reference to an FAQ that is on the TRM website, that explains that. Right? You know when the software is submitted to TRM and then when it's not. Next slide please.

Section eight. Agreements, authorizations, and contracts. This section is pretty straightforward. Will the research study have any agreements, authorizations, or contracts? That's a yes or no question. If yes, then you'll be asked to select the types of agreements and authorizations that will be used in the research study and if the research study will involve the use of a contract. So you do just select all that apply right there. And question three, you're just asked to describe the purpose of the agreement or contract and provide the names of each entity involved in the agreement or that contract. Next slide please.

And this training scenario here has got to do with contracts. The San Francisco VA is conducting a VA only research study and the PI plans to contract with an external entity to conduct electronic surveys of VA research subjects enrolled in the study. Should the external entities information system be submitted for a VA ATO determination? The answer is yes. So while you do have a contract or you're going to have a contract of an external entity, if that external entity is collecting, processing, or storing data on behalf of the VA, that system probably needs a VA authority to operate. And so that system would need to be submitted you know for that ATO determination if it needs an ATO or not. Next slide please.

Section nine, data sharing with external entities and external information systems. Will any research study data be transmitted or transferred to an external entity? Again, that's one of the conditions we've kind of covered that, it's a yes or no question. If any data will be transmitted or transferred, then you're asked to provide the name of the entity and describe the method used to securely transfer the research study data. Now this is section nine which is data sharing with external entities. Within this section we also provide you a list of the different ways that you can securely transfer that research data to an external entity. The third question is, will VA retain ownership of the research study data shared with the external entity? This is a yes or no question. The reason for this answer is, you know if we're sharing data with someone and we own that data, then in most cases VA securities policies apply and then you know then there's a lot of security controls that apply as well so. Will the research study use any external information systems, applications, or devices? And what external information system like the contract we just looked at, with an external entity that's going to be collecting research surveys for us, right? Their system is considered an external information system. It does not have a VA ATO. That also includes applications as well, or devices. Will those be used in the research study? You know that when we do have a lot of spots or clinical trials, you know this question here I've seen some studies where you'll have four or five different systems and applications as well as a mobile device, and a mobile app, so. Number five, who owns the data being collected, processed, or stored on the external information system? Now this may look similar to the one up above, and that's for the data that we're transferring out. Who owns that data, right? This is for the data that's being collected on that external information system. Now one thing that is coming out here soon, and I'm just going to just lightly mention it. You know there are systems out there that are collecting data. A good example let's say a Fitbit. So right now a Fitbit, let's say that that Fitbit is going to be used in a research study. You know who owns that data right? If it's a VA only study you would think that the VA owned that data, but they're actually, they're working on the guidance right now for patient generated data to determine you know is that really VA data, or is it data owned by the subject. Right? So but as it stands now that policy is not in place right now so I just wanted to give you a heads up that something like that is coming down the pipe here. Number six - select the type of external information system or application that will be used in the research study. These are the most common ones that we've seen. Some of these may look new to some of you. We noticed that when COVID kicked off and really the need for remote data collection really went up, right? We started seeing all these different kinds of systems we had not seen in the past. If your system is not listed here you would just select other and then provide it in the box provided. Next slide please.

And question seven you'd be asked to provide the name, the web address and the purpose of each information system or application used in the research study. One of the things that has had protocols returned back to the PI is their using an external information system, right? And we're going to be transferring information you know to that information system, right? The ISSO needs that web address so that they can verify that that connection is encrypted with FIPS 140-2, or it's successor validating encryption. Number eight, will an external entity provide mobile, portable storage, medical or research scientific computing device to be used in the research study? And that could be answered yes or no question. If it's yes, then a small box will appear, sorry I'm getting my ones mixed up. If the answer is yes, then it will ask you to select the type of externally provided mobile portable storage medical or research scientific computing device. That will be used in that study. If they aren't listed again, check other and then you'll be presented a spot to detail those devices. Next slide please.

Then you'll be asked to provide the make, model, owner, and purpose of each external entity provided mobile, portable storage, medical and research scientific computing devices used in the research study. And just to give you an example of this, I mean we've seen studies frequently that say that you know, we had one where it was a COVID study that if the subject got COVID-19 they would be provided a device for monitoring. Right? This is where question 10 comes in. You know what is the make and model of that device, right? Who owns it, right? And that's why these kind of questions are being asked. So because sometimes the protocols are not necessarily clear. Number 11, if any affiliate, now we transition to affiliates, if any affiliate mobile, portable storage, medical, research scientific computing device or laptop will be used in the research study, will the devices be used at a VA facility? Now this question may seem strange. Why are we asking will they be used at a VA facility? The reason is, in VA handbook 7000.2 which is logistics, if an affiliate device is used at the VA it must be added to a VA EIL and it must have a VA EE number assigned to it. That's why we're asking this question. Number 12, will the research study use any external entity provided mobile applications? Again, you know we're starting to see a lot of this now with remote data collection. If the answer is yes then you're asked to provide the name of the mobile app, the entity providing or creating the mobile app, website to download the app and the purpose of it in the research study. Next slide please.

So the San Antonio VA is conducting a collaborative research study with their affiliate university. Each research subject has consented to providing a copy of their study data to the affiliated university, but the affiliate university's eCRF application is blocked by the VA CSOC. So now the PI can't upload that data as planned to the affiliate. As a work around the PI plans to use a DSL internet connection located in the San Antonio VA research service that does not have a VA ATO. Can this system be used to transmit the data? The answer is no. You know we have seen and also heard about, there's a lot of VA facilities that have these DSL lines set up, you know have a little wireless system setup into sections right? They have a contract with the local cable provider, or the local phone company provider, but those systems have not been evaluated by the VA right? They don't have any security controls on them et cetera. So they cannot be used you know to transmit VA data or to store it. Right? So if it doesn't have a VA ATO the system is considered an external information system and cannot be used. Just as a

sidenote on that. I know they are working on a research wireless for most VAMCs for research use. You know for when you have sites that are blocked by the CSOC for whatever reason and it's difficult to unblock those, there is also a team working on that now looking at getting a research wireless in place for those situations. And I haven't heard for a while now, but I know that it was in a testing phase at three facilities here recently. Next slide please.

So now we're going to talk a little bit about amendments. When is an ERDSP required for a research study amendment? An ERDSP is required to be completed for all research study amendments. There's a slight caveat in that, and we're going to see it here in just a few minutes. Next slide please.

Again, how do you determine if an ISSO review is required for a research protocol amendment? So when you're completing that ERDSP for an amendment right? You're going to select amendment up top for the type of study. The branching logic kicks in and it's going to ask you out of these sections that we just reviewed will the amendment make any changes to any of these sections in the ERDSP. Right? If the answer is yes then you of course will select those sections. And we'll kind of get into that here in a second. When we're talking about if an ISSO review is required and this is something I didn't touch on previously for all the new ones, but whenever you know those research study conditions are selected as yes, or if there are, we also have embedded questions in the different sections, right? So let's say you marked all of those no, but then you go into one of the sections that mark a question as yes that's related to one of those study conditions, an ISSO review is required. So again this is a branching logic form. When you select one of those conditions as yes, or a question that has related those as yes, it will pop right above signature block a banner that says, an ISSO review is required. So the banner will always tell you when it's required or not. And just a sidenote, if the research study amendment is only making minor changes to the research study as well, the ISSO review is not required. Next slide please.

So we're going to go through these questions real quick, and there's only I think three of them. Will the amendment make any changes to any of the sections of the ERDSP? Like we just spoke about, that's a yes or no question. If they say yes, then you just select those sections that you're going to change, and then you go into those sections and you make those changes. Next slide please.

Okay. So remember that first question that said will the amendment make changes in the section of the ERDSP? If that is marked no, right? You know and again you know when would you mark it no? And I want to show you here in a second. But we have a table within the ERDSP guide that lists what minor changes are. Right? So if you had a minor change, a minor change will never make a change to any of the sections of the ERDSP right? And what I'm talking about here is, I've got a research study and we're going to recruit 500 people, 500 research subjects. We do an amendment because we decided we want to recruit 600. Again, that doesn't change anything in the ERDSP and so you would just mark it simply no. And then you would just complete the header information, that first question and sign it. That's it. And this would go in

with your IRB submission package, so the IRB and the R&D Committee it knows that an ERDSP is not required. Right? So that will let them know that. Next slide please.

And this is a screen capture of parts of the minor change determination aid. But we do have several things in here. Right? You know if you're making minor changes to recruitment procedures. You know materials. Or submission of new recruitment materials. You know minor changes to project documents like paper surveys or questionnaires or brochures. Right? Those are minor changes in the ERDSP that's not required et cetera. And we have, there are several in that table that is in the ERDSP guide. Next slide please.

In this training scenario a PI plans to submit an amendment to a VA research study. The amendment will change the number of subjects that will be participating in the study from 400 to 750. Is the PI required to complete an ERDSP? I kinda already gave it away when I was talking just now. So if it's only making that minor change, right, again you just complete the heading, complete question one as no, you sign it and then submit that with your protocol submission. Next slide please.

So let's walk through real quick locating that toolset in the VAIRRS as well as on the SharePoint.

Carol Johnson: Okay Terry, we're going to turn over the sharing capabilities to you for your demo.

Terry Peters: Okay, thank you.

Moderator: And Terry, just a reminder that there's 15 minutes left.

Terry Peters: Okay. Thank you yeah. I'm going to talk fast now. Okay, so when you go into VAIRRS you'll login to it. And then once you're in you just go to forms and templates here on your left. You will then see all the libraries up top here. We actually see them all, but you won't see this whole list I don't believe. And you simply scroll down. And you look for VHA ORPP&E and here they are. There's the four libraries. The Animal Committee, Human Subjects, Safety and Bio Safety, and the R&D Committee Members, that's where it's located. We also provided links as well back to the RSD public site. And of course this brings you right to the template user guide which are located right here. Also we also have them located as well on the ORD page in their toolkits. There's a research information security and cybersecurity toolkit. You would click on that and when you scroll down you would see the link right here to the template and the guide. So you do have three locations where you can go back and look for those. Okay, Carol, I'm going to stop sharing. Oh, I'm sorry, we're going to do one other thing and then I'm going to make this quick. So I know, I want to try to get to a few questions. There we go. So this is what the template looks like. When you first see it you will notice it's just one page. Right? There's no questions on it. What you do on there and we're just going to real quick, you would complete your header information, put in the title, the type of research study -Animal, Basic lab, Human or animal/basic lab. You would then select your VA facility. And again you notice there's no questions. And then once you select that purpose, that's when the branching logic starts. And

then it presents those conditions we we're just talking about. If you were to mark one of these yes, and all the rest no. You'll notice that it did expand out several sections for you to respond to. Now again, when you're responding in these sections, it doesn't mean that you're going to answer all of the questions in that section. You may only answer one or two of them. You'll then be asked to select the data classification of the study. You know in most studies you're going to have sensitive and non-sensitive. And then after you've determined your data classification, and we're just going to do collect for section three real quick. Does it involve more than one VA participating site, and we're going to answer yes to that. And then of course you provide the name of each of those sites. And you'll notice as we're going through here you know again like you saw the data sources right? You would pick those. You know if you pick other then it pops that box. So that you can put the information in, right? So this is the great thing about this branching logic. If you had no other and you're only going to use non-VA medical records, let's say, there's a question right there that you won't be answering. Right? So. And that's just kind of how the form works. Real quick, if you make a mistake in a section you can reset that section, or you can scroll down to the bottom and reset the whole form. You'll notice that we did mark one of the conditions, and a couple of the questions. And this is where an ISSO review is required by research study condition 1. And also by one of the questions that was answered in section two. So this way you always know if an ISSO review is required. Right? It's not subjective, the form will tell you. Okay. Carol, I'm going to stop sharing.

Carol Johnson: Okay. Thank you, Terry.

Terry Peters: Yes. There we go. I'm used to Teams. This has kind of got me. Carol you want to share them back out. I think we've probably.

Carol Johnson: Yes.

Terry Peters: Are we towards the end?

Carol Johnson: Yes. One moment.

Terry Peters: So I want to try and run through some of these questions real quick and get them laid out here. Okay. Yeah, and then in the slides here we also provided a link to the ERDSP feedback form that is also in the guide. So if you have any suggestions or things we should change or things that you don't feel are relevant, et cetera, please submit those to us. All feedback is certainly very welcome. And again we just talked about the importance of the ERDSP. We discussed the roles and responsibilities. You know a review of the ERDSP within the IRB and R&D process. We did review you know the phase implementation schedule. So right now it's only those 30 sites. We talked about determining when a study or a protocol requires an ISSO review. We reviewed the use of the ERDSP toolset. We covered several training scenarios. And we just did the demo as well. Next slide, Carol.

Okay. And at the end here, this is our last slide. Here's some references for you. Again, you know the portal where the template guide is located on our SharePoint, as well as we have

FAQs there. In VAIRRS, the VAIRRS portal as well as the VAIRRS training energizers. And of course the R&D research information and cybersecurity toolkit. Again, if there's ever any questions, reach out to us for help or support. Here's our DL. Please use that DL versus emailing individual people. Because when it comes in this DL it gets tagged in our system. Assigned a number and then it's tracked. So that way you know if it doesn't get lost in somebody's email box somewhere. Okay. I believe we're at the end now. Do we want to try to answer a few of the questions real quick?

Moderator: Yep. And I'll just take one moment to share my screen. And you should see the first question.

Carol Johnson: I think I just wanted to add to your last statement in terms of reaching out to our Distribution List. We do encourage you to work directly with your local ISSO as well. And any questions you have we also ask that you engage your local ISSO in those questions. So that it's a learning experience for everyone. So we appreciate that.

Terry Peters: Yeah. Good point, Carol. Yeah, and it keeps the ISSO in the loop so when you do submit that research study they'll understand why maybe a certain change is in there. Right. So. Is the research protocol amendment the same as a modification? For us in RSD I mean we've always seen them as research protocol amendments. Karen, if you're on.

Dr. Karen Jeans: Hi, this is Karen Jeans here in ORD. But yes, when there is a modification to the approved protocol that's the same thing as the protocol amendment. The use of the words are interchangeable. So the answer is yes.

Terry Peters: Okay. Thank you. I thought that, but I wasn't sure about that one.

Carol Johnson: Okay, I'll read this one.

Terry Peters: Yeah go ahead.

Carol Johnson: Okay the sites, this is from slide nine, the sites that are part of the soft launch, or ERDSP which will be providing feedback after 4/19, would you communicate those sites? What this evaluation feedback would look like, so the sites know what they're to be focusing on, assessing now while using it. Thanks.

Terry Peters: Okay. I think, okay yes. I think what we're asking here is during that soft launch, right? As we're getting feedback on the form, right? If there's some issues, will we be communicating that to the other participating sites? And that is yes. We will. If there's an issue that's going to affect you know the way that study is documented, is it a problem with the questions, a problem with the form, we would definitely be communicating that to the other participating sites to make sure they're aware of that issue.

Carol Johnson: Okay. Next question or maybe a statement. I strongly recommend not using the term VASI without defining it. What is VASI or VA Sensitive Information? Would you include examples. Following up on a prior question, VASI or VA Sensitive Information is defined very broadly in the 6500 and relatively narrowly here. Is the definition used in the ERDSP for the ERDSP ISSO triaging only? Or can we deidentify data as non-sensitive across the board?

Terry Peters: Okay, so what we have in the ERDSP template, the guide, right? We do have that table that identifies you know within research what is considered sensitive, right? And what is considered non-sensitive. And yeah, I mean you're right. I mean the VA Sensitive Information there's several different definitions of it out there. But we're pretty much, you know that was used in creating that classification table, right? To determine what was sensitive and non-sensitive in research. So again, that table was a collaborative effort with ORD as well as ORO. So you know that table is for use by all VA researchers in determining if their data is sensitive or not. And yes, deidentified data is considered non-sensitive.

Carol Johnson: Okay, thank you Terry. Can you give an example of a study that wouldn't involve accessing, generating, transmitting VA Sensitive Information? VA Sensitive Information has an extremely broad definition. I'm having difficulty imagining a research study that does not involve any such data.

DuJuan Williams: Okay. Yeah. I've seen a few in the past. You know again, we don't necessarily see the types of studies that are seen in a local facility. But I have seen some research studies involving a PharmD, who is the PI on the study. And they're doing a retrospective study. Let's say they're looking at the effects of Lisinopril, you know it's a blood pressure medication in individuals let's say over 65. Right? But they're taking data from two previous studies, or maybe one previous study, and using it in their study. But that data is deidentified, and they're not collecting any additional information. They're simply taking that information and then using it in their study. Right? So I have seen a few of those where there was no sensitive information involved. I mean it's pretty rare, I think. But they do have those in those retrospective reviews. Right? If they're using deidentified data then no sensitive information is collected in that study.

Dr. Karen Jeans: This is Karen, I want to add to this as well. Yes, we actually have quite a number of studies in which deidentified individual line data sets are received by VA researchers from numerous different sources. And these are studies in which you know they truly are only involving the receipt, the use, the access, the analysis of deidentified data. And that is not human subjects under the comparable. And so that does not involve VA Sensitive Information.

Terry Peters: Great. Thank you, Karen, thank you. Okay.

Carol Johnson: Okay thank you. Just wondering what percentage of studies are expected to not require ISSO review under this new approach.

Terry Peters: Right now, to be honest with you, we do expect you know to see the number of studies that they review to go down. But at this time, you know we don't have an estimate on

that. As to how many, you know what percentage of those studies are expected to not require an ISSO review. But we do expect that number that they currently review to go down.

Carol Johnson: Okay. We have been using the test version of the ERDSP since last year but are not included on the Phase I site list. So for now, would you prefer that we do not have researchers use the final version posted in the ORPP&E library?

Terry Peters: Yes. We recommend you not use that. Continue using the template that you currently have. And the reason is this soft pilot release phase is a short period. And we don't want you to start using a new form when we're going to turn around and update the form we currently have, right? To a final version by May the 10th right? So just keep using what you currently have. And then once it's finalized and it goes live for everybody on the 10th of May, then you'll use that new version.

Carol Johnson: Thank you, Terry. How are we doing on time? Are we okay with continuing?

Terry Peters: We've got about a minute or two, so I think we can probably get one more in.

Carol Johnson: Okay, so let's go through this one real quick. For the case with the external devices on the affiliate Local Area Network, LAN. What if those devices belong to affiliate universities, but are not connected to the LAN or any other network? Like standalone equipment that collects data.

Terry Peters: So on those devices you know they do need to be on a VA EIL to have an EE number assigned to them, for that use. And this is actually a good question and I'll be honest with you. We're actually looking into addressing this as if we've got a scientific computing device that's over at the VA. You know and we're using it to analyze let's say some tissue samples or whatever. How do we handle the use of external information system? Because we know that's frequently done in the labs, right? So we are currently working on some guidance for that. So I have to defer that question for now. But we will come back and give you a proper answer on that.

Moderator: All right, and it is 3:30. So we have run out of time. I want to thank everyone for all of the questions they've submitted.

Terry Peters: Great. And thank you everyone, I really appreciate y'alls time. I know you're all very busy and I hope everybody has a good afternoon.

[END OF AUDIO]