VA Mobile Discussion Series

April Webinar: What You Need to Know About Privacy and Security

VA's Mobile Discussion Series is a monthly webinar featuring a variety of topics focused around app development and mobile health at VA.

Micah Azzano: Hello everyone. Welcome and thank you for attending the Connected Care Discussion Series webinar. This month's discussion is VA Mobile Health: What You Need to Know about Security and Privacy. My name is Micah Azzano. And I'm going to run through a few, brief technical reminders before we begin. Your phone lines are muted, so we'll be taking questions through the chat feature. The chat function is available to you at the right of your screen. And if you're experiencing any technical difficulties, please use the chat and someone will be with you to assist.

If you'd like to download the presentation or other resources, you may do so by clicking on the file name below the chat screen. The full presentation will also be available at a later date on the Connected Care Discussion Series webpage. A few, quick disclaimers I want to go through before we begin, the following lecture is for internal VA educational purposes, and the views expressed are those of the authors and do not reflect any official policy. The authors have no financial conflicts of interest and references in this training to any specific commercial product, process, or service, or the use of any trade, firm, or corporation name is for information and convenience, and does not constitute endorsement, recommendation, or favoring by the VA.

Today, we welcome our presenters, Dr. Christina Armstrong, clinical psychologist, Connected Health implementation strategist, Office of Connected Care, US Department of Veteran Affairs. And Dr. Beth Jaworski, social psychologist, mobile app specialist, National Center for PTSD Dissemination and Training Division. Please note that we will be taking your questions periodically throughout the webinar. So, please type them into the chat at any time. And with that, I will turn it over to Dr. Armstrong.

Dr. Christina Armstrong: Thank you so much, Micah. And thank you all of you that came today. This is a really interesting topic, and I know one that a lot of people have a lot of questions about. I'm happy to have you here. We're recording this too, so people can see this later on as well. Many of us use mobile health apps and other health technologies to provide easy access to healthcare and health resources. The security and privacy regarding our digital data is one of the most important topics. But it's also one that can be confusing, and a matter of significant concern for providers and patients alike. Today, we want to break down this topic for you regarding mobile health apps in order to clarify what you need to know, and how to communicate security and privacy issues to your patients.

Our goal by the end of this training is that you'll leave feeling comfortable talking with others about the differences between different types of apps, and how they handle the security and privacy of your health information. If you'd like further training, there are many opportunities available to you via the VA's talent management system, several of which we have listed here

for your convenience. Understanding mobile health security is important for providers and patients, not just because of the laws protecting patient data, and ethical codes for clinicians but also because concerns related to security and privacy are one of the biggest barriers to adoption of virtual health tools for providers and patients.

So, we need to be able to inform providers and patients how the data are being used before they can feel comfortable using the products. Now, although, mobile health has really only been around a little over a decade, when it comes to the delivery of healthcare, most of what we're doing is actually quite the same, which is delivering evidence-based care. So, while the delivery mechanism for care and information has changed, we do have a strong foundation of policies, guidelines, and laws in place to protect our health data. So, these, of course, include, privacy apps, HIPAA privacy laws, HIPAA security rule, high-tech facets, 2009, and also many organizational policies as well.

Also, for those of us that are licensed providers, newer ethics codes and standards include information about this topic. So, while these policies and guidelines provide us a solid foundation for our understanding, it is still confusing for many and can be difficult to translate it into clear and simple language so that providers, and patients can make informed decisions regarding which technologies to use or how to best protect their health data. Now, research shows that mobile health can effectively supplement medical care. It does this by overcoming barriers to accessing care, increases patient compliance with treatment, and also increases their engagement in care.

That also supports the facilitation of case management across geographic locations, and helps extend healthcare beyond face-to-face visits. And certainly, in the time of Coronavirus, we are seeing the benefits of these virtual health technologies shining brightly for everyone to see. We need these to do our jobs. Our patients need them to be able to receive care. So, having said that despite all those benefits, we've also seen barriers in the adoption of mobile health. Concerns about data security and privacy are consistently seen as one of the top barriers to adoption across multiple studies. And so, you can see here, here's an example just of three studies but there's many, many other examples.

So, this is a top issue for patients and providers. And so, we want to discuss that. Okay. So, what does the staff need to know to be able to break down those barriers to adoption? Certainly, being able to identify and problem solve regarding security and privacy issues is one of the core areas of competence when you need it. However, when looking at the bigger picture, there are several other areas of competence, and use as well. And these include having an understanding of the evidence space, knowing how to integrate these technologies into clinical care, and having an understanding of ethical issues, and also cultural considerations.

When we're looking at the big picture, these are all the pieces that we need to know. However, although, I'm giving you this bigger picture to provide context for you today, today we will focus on security and privacy. And there is great information available. We have some references there, and we have some files available in the files pod there, it's free to download, if you want

to learn more about these other areas of competence. Okay, well, there are many great mobile health apps out there. It can be really confusing how data security and privacy is handled for those apps not developed by the federal government.

For mobile health apps developed by the federal government, strict standards for data security and privacy are in place, and are required at every step of the development process. And the way that the data is handled is clear, and much easier to explain. And so, for that reason today, we're going to focus on apps developed by the VA. Although, we'll give some other best practice tips for non-government apps later on. So, here on the screen, you can see the go-to place for all information on all of the VA mobile apps that are available, which is mobile.va.gov. And Micah can show ... Yep. She's way ahead of me. And so, here, you'll be able to filter for apps for veterans, apps for the staff, and also based on what platform they're available on.

Here, you'll also see what apps are available for download on the Apple app store for Apple devices, and also those that are available from the Google Play app store for Android devices. There's also web app, that are in the app store that launch directly from that page there. So, this is really the go-to place where you can find information. And we also have some other tools in the files pod that helps you get a good idea of what's available, what platforms, what conditions are they used for? And that's the virtual tools guide for clinicians. That's the decision support tool for the staff, and also the prescription pad, which allows you to communicate with patient which tools you've identified for them.

So, those are two tools that we've developed that we hope are useful to all of you. Okay. So, for all of VA apps, the data is securely protected. It enables you to use our app to improve your health, and wellness without concerns for privacy. So, while all apps keep personal information secure, some apps do so in different ways than others. Where the data's stored and who can see it is different based on whether a VA app is a connected app, or a self-contained app. So, examples of self-contained apps includes PTSD Coach, which is been downloaded over half a million times, and also the brand new VA COVID Coach app. So, these are examples of self-contained apps.

Examples of connected apps are virtual care managers, and the Annie app. So, how do you know which apps are connected, and which ones are self-contained? Connected apps have a little lock icon on the lower right hand corner of the app icon. So, now I will hand it over to Dr. Jaworski, and she's going to discuss more about VA's self-contained apps.

Dr. Beth Jaworski: Alright. Thank you, Dr. Armstrong. So, I'm going to be covering the VA self-contained mobile mental health apps made by the National Center for PTSD. A few key things to note, they are private. They don't collect, or require any personal identifying information. You don't need to create a user account. You can just download them, and start using them. They are self-contained, meaning that they do not connect with the VA's electronic health record. And you own the data, and you can delete the app at any point in time. These apps are free, and they are available in the Apple app store, and the Google Play store.

They are 508 compliant, meaning that they're accessible to individuals with disabilities. So, for example, all these apps work with VoiceOver, or TalkBack for those with vision impairments. And additionally, these apps all contain interactive tools, crisis resources, ways to track progress, and psychoeducational materials that are evidence-informed. The self-contained app, typically fall into one of two main categories. Those that can be used for self-care, and those that are designed to be used in conjunction with treatment. So, the self-care apps that are highlighted here are PTSD Coach, our flagship app.

And the first one that came out, PTSD Family Coach, Mindfulness Coach, Mood Coach for behavioral activation, Aim for anger and irritability management, That Change for alcohol reduction, Concussion Coach for concussions, and mild traumatic brain injuries, Moving Forward for problem solving, Parenting2Go to develop skills, to help parents connect with their children. And as Dr. Armstrong mentioned our newest app, COVID Coach, which was just released a few weeks ago, and is designed for stress management during the COVID-19 pandemic and beyond. And it's also available for both iOS and Android. The treatment companion apps you see here include PE Coach, to support prolonged exposure therapy, CBT-i Coach for cognitive behavioral therapy for insomnia.

CPT Coach for cognitive processing therapy, ACT Coach for acceptance and commitment therapy, STAIR Coach for skilled training in affective and interpersonal regulation, and Stay Quit Coach for tobacco cessation. We had previously thought that we would be able to share this video, but we decided that it might be best with video quality, and other potential tech issues, to just highlight this video, and share the link in the chats. This is a great resource featuring Dr. McGee Vincent, and she demonstrates how to cover some security and privacy concerns, using PTSD Coach as an example in a clinical setting. And now I will turn things back over to Dr. Armstrong.

Dr. Christina Armstrong: Thank you so much. Yeah. In this video, I want to urge all of you guys to take a look at that, check out this. And there's also a whole suite of similar videos. This one's specific to security and privacy. And often patients will ask you questions about, "Who can see the status? Where does it go?" And so this is a video, a very short video, I think it's about five minutes showing Dr. McGee Vincent having a conversation with ... It's an actor veteran, not a real veteran, but having a conversation as the veteran asks questions, and how a provider should respond.

And so, that is specific to the self-contained apps, but a similar type of process can be done with other apps too. And I also want to highlight in the files pod, there's a mobile health practice guide. And there is also a script for giving you an example of how to have that conversation. And the mobile practice guide looks like this, but, of course, it's available for download in the files pod for you. Okay. Moving along. Alright. So, those are the self-contained apps. They're self-contained, they're like a little sandbox. They're not connecting to the VA network at all. They're on their own. VA cannot see what's in there. However, we have a whole

different set of apps called connected app. VA connected apps. So, connected apps are apps that connect to the VA's network.

So, additional data security is required to help ensure protection meets strict federal standards for your personal health information. These apps requires secure user authentication, such as if you're a veteran, you can use your My HealtheVet log in information, or a DS Logon credential. If you're a staff member, you would use your PIV card. This authentication process then allows us to be able to securely share information with your healthcare team. Alright, let's look at some of the VA connected apps for healthcare professionals to start with.

These apps require authentication to log in. So, VA PIV, or PIV exemption, or Vista login credentials for VA staff. So, you can see some of the apps here that I want to highlight. So, Virtual Care Manager, I'm sure that a lot of you guys have heard of, used, especially, during the COVID pandemic. This is one that we've seen a lot more use. Also, ME app for clinicians. This is text message protocols that the staff can go in and prescribe to patients for all different conditions. We have now released several, for Coronavirus too. And also we have some, including one of those Coronavirus protocols for Annie that are veterans self-subscribed.

So, veteran can log into Annie app for veterans, and going and self-subscribe. And that is what I have done. And I now receive any Coronavirus precautions texts, and I love it. It's just a great way to get up-to-date on all the information you need to know, and make sure you're staying well. So, for VA staff to access connected apps, they need to link their PIV. So, that's one option. And so, if you need information on how to link your PIV. We do have a PIV linkage guide. It's available in the files pod for you to download. And we also have a link here for you.

And is on mobile.va.gov. So, we always update it if it needs to. So, that's the best location for it. Also, for those of you downloading things from the file pod, I got a pro-tip for you. In the files pod, in the upper right hand corner, you'll see stack of tiny lines, and a little upside down triangle. If you click on that, you can click download all, and you can download all of those files all at once to your desktop. Here's some veterans facing connected apps. Veterans can log in via three different methods that you can see here to the ... Actually it doesn't show it here, but I'll show you on the next page. So, you can see here.

But let me go back for a second, and we'll talk about it a little bit. So, some of these are ... So, I'd like to highlight, again, some of the apps, VA Video Connect, Annie, and Prescription Refill, but also the three VAs were used quite a bit before COVID. They have become indispensable tools during COVID to provide access to remote care, and self-management tools. Also, I mentioned before all of the different Annie protocols. We have I think 43 Annie protocols that are nationally approved. And topics that we have protocols on are hypertension, Coronavirus, relaxation, all different types of things that I think can be useful for most people, diabetes, [inaudible 00:24:20].

Also, I want to highlight a couple of other things. Prescription refill, you see there on the bottom, use of this has really taken off, as you can imagine, as people have to stay home, and

getting access to your medications is so critical when you're stuck, and you can't go out. We just released on Android, and now it is available on iOS. So, for Apple devices, and Android, so it's available on both platforms now. I know that it's in high demand for that to get out. So, we're happy to have that finally released. Also, coming soon is My VA Images.

We've been doing field testing, lots of research on this, but this would be the veteran stage thing side, and allow veterans to upload images, and photos and video of whatever medical issue that they have and be able to share that with the provider. And then, so the provider would access that information through Patient Viewer app, which is also a connected app. So, out of those three log in options for veterans to access connected apps, My HealtheVet premium really is the ideal method. This will allow veterans to not only access all the important features in my healthy vet, like prescription refills, and care messaging.

But it will also be an easy, and safe way for them to log into all those connected apps. So, then easier than having to know all kinds of different passcodes, and login information, we all know how hard that is, but then you get at My HealtheVet premium account, which is free, and then that allows them to log into all of these. So, if you want to learn more about how you can help veterans in upgrading their My HealtheVet account, a link is included here for more information. And with that, I will hand it back over to Dr. Jaworski

Dr. Beth Jaworski: Thank you, Dr. Armstrong. I would now like to cover a few topics related to be an informed mobile health user, whether you are using a VA or a non-VA app. Although, the examples I draw will primarily be from VA app. One of the first things to consider before downloading an app is who developed it? Was it built by a government agency? A for-profit company, an individual, or some other entity? That's a question you should be able to answer about the app. And if you are uncertain, or you have questions, it's good to use known and reputable websites, or other trusted sources of information to find out more about the app, and the developer.

For any of the self-contained mobile mental health apps, for example, you can look up detailed information about the app, their privacy policies, and can find more information about them on the National Center for PTSD website. You can trust that we aren't making money on the app, and we are not collecting or selling any personally identifying information. It's important to know that sort of information for all of the apps that you download and use, but especially, health-related apps. And even when you are dealing with apps from trusted sources, there may be some privacy and security questions that come up. Like for example, permissions.

We frequently get asked questions related to permissions. So, I'd like to spend just a little time going over those, and providing some examples. So, many apps ask for permission. And as long as you trust the developer and understand the reason for the request they're okay to grant. One of the advantages of creating apps rather than mobile friendly websites for health is that apps can be made to allow the user to personalize their experience with information from their device. So, we tend to keep things like music, photos, calendars, and personal contacts on our device. And this content can be used to add personal touches to the app.

Mobile devices also have built-in cameras and microphones that can be used to create content. And being able to leverage these device functionalities was by device manufacturers. They built these capabilities in from the beginning, in order to make apps and app development more appealing. And so, these connections are built in secure ways. Before you grant permissions in an app, you should make sure that the developers clearly explain why they need the permission, and you understand the request. And it makes sense with respect to the purpose of the app.

For Android devices, it's a little bit more difficult to do. The explanation has to be custom built. So, you may have to rely on context. And sometimes Android apps, depending on the way they're built might ask for permissions on first use. And so, we're working on this to try and improve it, and make those permissions process more clear. For Apple devices, Apple has set aside a text field for this in the permission requests, and requires any new apps to include this explanation in plain language before they will approve an app to the app store. So, in the next few slides, I'm going to walk through what some of these permissions look like, using PTSD Coach as an example. Here's an example of how PTSD Coach for Android handles permissions when you first download the app.

In this case, you can see, it says, "Allow PTSD Coach access to photos, media, and files on your device." And your choices are to deny and allow. And that's a little bit much for some people. They're wondering why is the app asking for permission to all of these things. And as we've gotten some questions about this, if you say deny on the screen, it looks like you can't use the app. And there is a workaround for this. It's not ideal. And again, we are working on making this process clear, and more transparent. Suffice it to say, the reason that it needs access to the files on your device is it really needs access to the storage because PTSD Coach has a lot of additional files for Android that are downloaded separately.

And those help you use the audio guided exercises within the app. And also, if you're using PTSD Coach in Spanish, it allows you to access the Spanish language version. You do not need to grant access to the camera, the contacts, or microphone on the device, in order for the app to work, but on Android that's not as clear. And we're working on that. I'm going to move on to iOS where things are spelled out a little bit more clearly. And it's a little bit easier to spell things out. So, I'll start with a question that we get often about why is the app asking for access to my contacts? So, in this case in PTSD Coach, if you go to crisis resources, and you want to add a contact to your personal support list, and you do this for the very first time, you see this permission that says PTSD Coach would like to access your contacts. In this case, if you don't allow access, you won't be able to add people from your contacts app to your personal support list.

Another example is with respect to notifications, the first time you set a reminder in the app, whether to take an assessment, or get a daily inspiring quote, and you see a permission about the app being able to send you notifications and badges. And again, you can choose to allow or not allow. With respect to the camera, here's another example. You are able to customize a

tool in PTSD Coach with your own photos. There are stock photos that are included with the app, but if you choose to add photos, for example, you want to use your camera to take a photo of something while you are using the app, you decided this would be a great photo to add. You can allow the app to access your camera, and take a photo, and then save it right into this tool.

Similarly, if you would like to upload photos that you have already taken into this tool, you need to allow the app access to your photo library. And here's an example of how you can review your permission. There's something similar for Android, but in the case of iOS, if you go to the settings app on your device, you can see which permissions you have granted, you can always update them. And in this example, you don't see contacts on this list because the screenshot was taken before I had added the contacts. So, once you grant something permission, then you see it on this list, and you can always disable it.

And if you find that something isn't working within the app, it may be good to check out the settings, and make sure that if the permission depends on accessing certain information that you haven't granted permission to, such as you're not allowed to add a custom photo to the tools, you want to make sure and check that you've granted permission. Where are these data stored? That's another question that we often get. For the self-contained mobile mental health apps. These data are only stored on the device. So, the first line of defense for protecting these data is to set a device passcode. Personally identifying data are not shared with the VA, or any third party vendors.

In some cases and only where app users have provided permission, we capture some very crude metrics about how, and how much apps are being used in terms of things like which tools were used, which learned topics were viewed? But we have no identifying information. If you do have Cloud backup enabled for some apps or all apps on your device, then the updates are included with the devices regular backup that it encrypts and sends to the backup servers. So, things like iCloud for iOS. And this is necessary if you end up needing to get a new device, or you have to reset your device, then you're able to retain the data that were already stored in your app.

For majority of our apps that have been updated recently, you can access information about the privacy policy directly within the app. So, if you look at we call the lateral menu, the three lines in the upper left corner, you can access the menu. And then you see a section dedicated to the privacy policy. Any app that Apple or Google now allows in their app stores have to have a privacy policy separate from the user license agreement. And it usually has to be hosted on a website. It's important to take a look at it, if you understand what it's saying, and that you find the terms acceptable, and you know what your data will be used for.

Even if the app is from a government, or a nonprofit organization, look for any data sharing arrangements, some apps may be a public private partnership that do share data. So, it's good to just be aware. And then for the self-contained mobile mental health apps, there's also

information available on the National Center for PTSD website related to the privacy policies. And with that I will turn things back over to Dr. Armstrong.

Dr. Christina Armstrong: Thank you. Okay, so to recap what Dr. Jaworski is discussing, the key questions to consider when evaluating mobile health app safety, security and privacy, first of all is who made the app? And we know that for VA/DoD app, that is all the data is safe, secure, your information is kept private. So, that's important to know. But just in general it's important to be thinking about who made it, and also, what data are collected, and where are data stored? And also who has access to the data? And how can that data be used? And what are the alternative options for using a virtual care tool? So, for example, if you're using a self-contained app, like the PTSD Coach, the VA made it.

The data that's collected is whatever you put in the app, whether it's uploading, or getting contacts, things like that. But we can't see any of that. It's stored there in the app. And if you delete the app, that data is gone. We don't have a backup. And once you back it up in your iCloud, we have no access to it. And so your provider can have access to it. However, if you do want to share your information from those self-contained app, there is a really good process you can use. You can export all the data to yourself, and then send it via secure message to your provider. And we have a guide in the downloads pod there, it walks you through those stats, right?

And also, so what are the alternative options to using a virtual care tool? Because all of these tools are based on evidence-based practices that we use already, there are always an alternative option to using it, right? So, if you're doing prolonged exposure therapy, you can always use this paper pencil version of it. And that's fine. We all have options, and we just want to be able to meet our patients where they are at. And if it makes it easier for them, a virtual care tool is a great option. For those connected apps, again, VA makes them. Whatever data's collected in that app, Annie or anything like that, it's collected and it's stored on the servers. So, it's stored in VA servers, and it is protected based on federal law. And then you, who has access to the data, sometimes the providers can go in and see, like patient viewer, your provider would be able to go in and see the information that you upload through my VA images.

Also, so, for Annie's, the Annie for clinicians app, the providers can go in and see, but also the veteran can go in the Annie for veterans app, and also see their information too. And always there all these alternatives to a virtual care options. Okay. So, while VA mobile apps use the highest level of security to protect your information, you also have an important role to play in keeping your private false data secure. So, let's discuss some recommended privacy, and security practices that can be used for all mobile health apps and devices. Okay. So, what about all these terms? Like encryption, firewall, VPN. These are terms that everyone's a lot more familiar with now because a lot of people are working remotely than they didn't before.

But there really is a lot of terminology, the technology that can be confusing. However, you don't need to be a technology expert, or memorize all the terms to be able to protect your data, help your patients protect their data. Having a one page handout available when a patient

asks about how they can protect their information when using mobile devices can help you be more prepared. So, you can see this right here. I have dispensed out, you see it up there, it looks really small on the screen, but it's also available in the download pod. So, this hand that you can screen is available in the files pod, and describes the key ways that patients can protect their health information on mobile devices.

And it also describes in simple terms things like encryption, firewalls, VPNs. And what I like to do is I just like to have a stack of these printed. And when somebody asks about data security, I take it as an opportunity. "Oh, you have a question about data security? Wonderful. Let's talk about it." What you don't want to do is say, "Oh, you've got a question about data security. Oh, it's fine. Don't worry. Don't worry." That's not how we want to approach it. We want to listen to concerns, and be able to address them. So, what I do is I like to pick up this sheet and say, "Oh, okay, I hear their concerns." And then I say, "Oh, you're talking about encryption it sounds like." And then I'll actually circle that box, and I'll describe. And it has in simple terms what encryption is, and then how they can use that to protect their information. And then I just like to hand this to them so then they have a sheet as a reference.

So, then if there's other concerns that they have, that's great, but then they leave feeling heard, and that they do now have the tools and information they need to protect their information. Very, very important. So, some of the top ways that any of us can protect our health information on a mobile device, I mean, a lot of the things seem relatively simple, but sometimes simple is the best way to start. Right? So, let's go through a few. The number one way is through password protection. Not only should you have a password to protect your device, and your devices, like your phone, and tablets, but you may also want to have a password protection on some of your apps.

A separate password to provide an additional layer of security. So, that way if you let your four-year old, or in my case, eight-year old, and 11-year old play with your phone, they are prevented from going into individual apps that you don't want them to have access to. So, maintaining control of your device is also an important privacy precaution. But what do you do if you or your patient loses their device with their health information on it? So, first step, do not panic, right? There are ways to remote disable device to protect your information, or for your patients to protect their information. So, it's good to know that. I've had patients call in a panic. And so, being able to just know this exists, and that it's really easy to do is great.

So, the device manufacturers, including Apple and Android now make this very easy. There used to be some extra steps involved, but no longer. And you don't have to install anything. So, all you do is search for iOS, which is Apple products on erase device or Android erase device. And you'll find the manufacturer's instructions for that for your device. Okay. So, another thing people think about is public Wi-Fi. So, there's different layers of security, depending on what type of Wi-Fi you're on. if you are in just a wide open, there was no log on information, anything for Wi-Fi that you're on, that basically means anybody on that, that same network is possible to link in and view what you have. And it's not all that hard.

However, the next level would be if you go to Starbucks or something, and there does require some log in, there's some splash page where you have to log in. Now, that does provide a minimum level of firewall protection. But still you're within the same firewall as everybody else that's using that same network. So, there's still possibilities of things getting taken. So, if you're ever concerned you can turn off your sharing. You can also just shut down your phone, or your devices. You can also use it as your firewall. So, go into your settings of your phone and check that out. And also enable VPN, which is a Virtual Private Network. So, then it really is your private network, and nobody can access it.

And then when, in doubt, put your phone in airplane mode, and turn Wi-Fi off when you're not using it. However, know that all of the apps for the VA, they are encrypted. So, even if someone were to be able to get into your device, there's still layers of protection before they could even get into any information on those apps too. Also, with your banking app, for example, they might be able to get into your device, but it's going to be pretty hard to be able to get into that. Okay. So, we want to provide you all the resources available so that you feel comfortable, and that you know where to go if you have any additional questions.

This is a list of resources about security and privacy from the federal government. So, please check these out. I think they're really useful tools. And also we know that things change quite a bit. We have a good foundation of policies, and laws, and guidelines, but this is a changing landscape. So, know that these resources update often, so that you can access updated information when you need it.

Dr. Beth Jaworski: I also want to highlight.

Micah Azzano: [crosstalk 00:48:20].

Dr. Beth Jaworski: Yeah.

Micah Azzano: So, I just want to jump in real quick here. Just in the interest of time, we're going to want to get to questions here in a little bit, but I just want to remind everyone that if you do have questions to enter them in the chat. We'll get those started in just a few minutes.

Dr. Christina Armstrong: Great. Thank you, Micah. I want to highlight a video series on mobile health security that's available on healthit.gov. Again, just like the link that you saw earlier, this is an excellent, the [inaudible 00:48:50]. These are everything that you really need to know in a way that's helpful, and easy to explain to others. So, key takeaways for today are, you have a responsibility to understand and discuss issues relating to security and privacy with your patients.

So, for apps that don't require user authentication, VA only has access to aggregated data. We don't know what's in the app at all. For apps that connect to the health record, the VA does have access to that data, but it is protected by [inaudible 00:49:22] laws and regulations. And

with that, we hope that clarifies a lot for you. And I look forward to hearing the questions that you have.

Micah Azzano: Thank you, Christie. And actually we have one that just came in. Just, can you talk a little bit about caregivers and privacy, and what special considerations are there with access to apps and data for caregivers?

Dr. Christina Armstrong: Yes, I'll jump in, Dr. jaworski, you probably have some tips on this too. So, first of all, for all those self-contained apps, anyone in the world can use those. Anybody can access them, use them. Caregivers, please use them. There's actually quite a bit of resources available specifically for caregivers. Also, for the connected apps too, there are apps and resources available for caregivers. It depends on whether you need access too, and things like that though. Because they may have to have a release of information depending on the legal situation with that family. But I'll hand it over to Dr. Jaworski. And you're on mute.

Dr. Beth Jaworski: Thank you so much. That was a fantastic answer Dr. Armstrong. I think the only thing I would add is that for specifically among our self-contained apps, I would recommend PTSD Family Coach as a great resource, with a lot of psych education, and links to outside resources.

Micah Azzano: And tagging on to that whole resources stuff. There's a lot of great resources that have been provided throughout this presentation. Where would you recommend people start, and working their way through if they're new to this, and really want to dig in, but want to know where to begin?

Dr. Christina Armstrong: I'd recommend the first stop, it would be mobile.va.gov, or telehealth.va.gov. Those two sources are the go-to places for a great deal of this information. Another one is My HealtheVet. So, I'm blanking on this, but it is just right back a couple of sides. But those are the three go-to places if you're looking for virtual healthcare tools. When it comes to mobile health, I do recommend going, and kicking the tires. If you have not downloaded an app, download one, download PTSD, Coach, download COVID Coach, and check it out. Check out the privacy policy for yourself.

It's really good to see what it feels like to get that permission pop up and have to make the decision allow or not. And so, when you go through that process, you can better be able to help support your patients making those decisions too. If you've downloaded lots of apps before. Great. Pick another one that you have not ever heard of and download that too. [crosstalk 00:52:30]-

Dr. Beth Jaworski: I think the only thing I would add if you are specifically looking for information about the self-contained mobile mental health apps, I might also recommend myvaapp.com as a resource, specifically, for those apps.

Micah Azzano: Great. Thank you both. And I see some other people typing in some questions, so I'll give them a moment. And while we're waiting, quick question, we talked about setting up your settings, and how you can do that for data and information. Let's say you go in, and you set them, and then you decide you don't like those settings. When you go back and switch your settings, what happens to data information from there moving forward?

Dr. Beth Jaworski: If I understand the question correctly, if you go into the app and disable the option to submit, for example, anonymous usage data. From that point forward, it will look like people have stopped using the app, or that person has stopped using the app. So, we will no longer be seeing that data. And I would know if it reassures folks each time an app is downloaded, a brand new app is downloaded, it's assigned just a random string of letters, and numbers as a code. And so, we would just stop seeing data for that particular code once you turn that off.

If that question is in reference to what happens if you go into the settings app on your device, and you say, for example, "I no longer want the app to have access to my contacts, or my photos, or my camera." You'll still be able to use the app. You just may not be able to use certain features within the app anymore.

Dr. Christina Armstrong: Yeah, and one thing, a common misconception I think people have about those permissions is that, so if I say I give permission to my contacts, it isn't like PTSD is always searching through my contacts. Not at all. It's only when it's doing that one function. So, when I'm adding that contact, it'll say, "Okay, now I can do that." So, it really doesn't impact if you shut off those permissions through the settings app, it doesn't impact the functionality of the app except for if you're doing that one functionality. But yeah.

Dr. Beth Jaworski: Yeah. That is a great point. And I think it's also really important to highlight for people that have questions about things like photos, this question has come up. Does the VA have access then to your photos if you grant permission for the photos? No, we do not get your photos, that is just allowing PTSD Coach to pull photos into the app. Yeah.

Dr. Christina Armstrong: Just the photos you choose, and just at that time that you're pulling it.

Dr. Beth Jaworski: Exactly. Yeah.

Dr. Christina Armstrong: I mean, yeah. And that's the thing when it came to choose a trusted app, VA's the trusted source, so we know exactly how these apps are working on the back-end because we create them. But it is harder to say for other non-government app what's happening.

Micah Azzano: Alright. I see there's still people typing, but I'll just go ahead and ask if you guys have any final thoughts that you want to share with the group, Dr. Jaworski, I'll start with you, and then we'll go to Dr. Armstrong.

Dr. Beth Jaworski: Thank you, Micah. I don't think that I have anything further to add other than if people have any questions or concerns at all, please reach out to us at mobilementalhealth@va.gov.

Dr. Christina Armstrong: And I'd like to add that, I hope this clarifies a lot of questions people have. When we were creating this training, we thought, "What are the most often questions we get about this topic? And how can we break this down to make it simplified in a way? To make sense and not be so scary?" So, hopefully, we accomplished our goal today, and know that we're open if you have any questions. We want to be as transparent as possible.

Micah Azzano: Yeah, so, I absolutely thank you both did that. I want to thank you both Dr. Armstrong, and Dr. Jaworski for joining us today. I don't see anyone else typing any questions. So, in the chat right now, I'm going to put in a link to a survey. You can fill it out, just let us know how we're doing, but also you can propose topics for-