**NWX-HHS-FDA**

**Moderator: Irene Aihie**
**October 29, 2014**
**1:00 pm CT**

Coordinator: Thank you for standing by. At this time, all participants are in a listen only mode. After the presentation, we will conduct a question and answer session. If you would like to ask a question, you may press Star 1.

Today's conference is being recorded. If you have any objections, you may disconnect at this time.

Your host on today's call is Ms. Irene Aihie. Thank you. You may begin.

Irene Aihie: Hello. Welcome to today's FDA Webinar. I am Irene Aihie of CDRH's Office of Communication and Education.

Today, we will be discussing the final guidance document titled "Content of Premarket Submissions for Management of Cybersecurity and Medical Devices" which was published on October 2. The guidance applies to premarket medical device submissions received beginning October 1, 2014. This guidance identifies issues related to cybersecurity that manufacturers should consider in the design and development of their medical devices and in preparing premarket submissions.

The need for effective cybersecurity to ensure medical device functionality and safety has become more important with the increasing use of wireless, Internet and network connected devices, and the frequent electronic exchange of medical device related health information.

Today, Dr. Abiy Desta from CDRH's Office of Device Evaluation will present an overview of the guidance document. After the presentation, we will host a Q&A session during which Abby will be joined by the CDRH subject matter experts.

Now, I give you Abiy.

(Dr. Abiy Desta): Good afternoon and thank you for taking part in today's Webinar on FDA's recently published guidance on content of premarket submission for management of cybersecurity medical devices.

The purpose of this Webinar is to discuss the agency's recommendation on how companies should document their approach to managing cybersecurity risks on vulnerable medical devices and be a premarket submission. I will attempt to clarify FDA's recommendation and answer questions related to this guidance.

As background, this guidance document contains the FDA's current thinking on managing cybersecurity risks. It should be viewed only as recommendations by the agency. Companies may choose to implement a different approach to mitigating cybersecurity risks on their medical devices.

Medical devices like other computer systems can be vulnerable to security breaches potentially impacting the safety and effectiveness of the device.

This vulnerability is dramatically increased as more and more medical devices become connected to the Internet, hospital networks, and other medical devices.

To the extent to which security controls are needed will depend on device intended use, the intended environment of use, the type of cybersecurity vulnerabilities, the likelihood the vulnerability will be exploited, and the probability that the exploit will cause risk to patients.

FDA recognizes that medical device security is a shared responsibility between stakeholders including healthcare facilities, patients, providers, and manufacturers of medical devices. The agency recommends the instructions of use and the product specifications of a medical device include information on what cybersecurity controls are expected and the intended environment use.

This guidance is applicable to premarket submissions for medical devices -- I think I'm one slide ahead. I apologize.

This guidance is applicable to premarket submissions for medical devices containing software, program logic, or standalone software for the medical device. Types of submissions that this guidance applies to are premarket notification De Novo submissions, premarket approval, product protocols, and humanitarian device exemptions.

The agency recommends that medical device manufactures provides justifications in their premarket submission for security functions chosen for the medical device.

Examples of security functions manufacturers may choose to consider include: Limiting access to the device to authentication users; Terminating sessions after a set period of time where it is appropriate for that use environment; Using a layered authentication methods;

Using appropriate authentication; Strengthening password protection; Taking steps to minimize tampering, and requiring authentication before permitting updates; Implementing features that allow for security compromises to be detected, recognized, logged, timed and acted upon during normal use;

Developing and providing information to end users concerning appropriate actions to take upon detection of cybersecurity events; implementing device features that protect critical functionalities even when device cybersecurity has been compromised; and providing methods for retention and recovery of device configuration information.

The documentation that the agency would like to see in the premarket submission includes: Hazard analysis, mitigation, and degsine consideration pertaining to intentional and unintentional cybersecurity risks associated with your device;

A traceable matrix that links your actual cybersecurity controls to the cybersecurity risks that were considered; A summary describing the plan for providing validated software updates and patches as needed;

A summary describing controls that are in place to ensure that the medical device software will maintain its integrity while it is under your control; Device instruction for use and product specifications related to recommended cybersecurity controls appropriate for the intended use environment.

The agency has and will continue to recognize appropriate consensus standards on this topic. On Page 7 of the guidance document is a list of recognized standards. A link is also available where you can periodically check for updates on the recognized standards.

I would like to emphasize again manufacturers may choose to implement alternative approach for cybersecurity controls. If you do so, the agency asks that you provide the rationale for the appropriateness of the approach that you have chosen.

As you all know, cybersecurity threats are continuously evolving. The FDA would like to stress the importance of having a plan in place to appropriately manage these evolving threat landscapes.

Thank you. I am now ready to answer your questions.

Coordinator: If you would like to ask a question, please press Star 1on the phone at this time. Again, to ask a question, please press Star 1 and record your name when prompted. One moment please for your first question. One moment please. Our first question is from Boston Scientific. Your line is open.

Man: Hi there. Regarding the mitigation of cybersecurity risks, is it adequate that the mitigations chosen to reduce the risks were selected in order to arrive in an acceptable residual risk for the system or does each risk have to be mitigated individually?

(Dr. Abiy Desta): Could you restate the question? I'm not sure I fully understood it.

Man: So you do a risk analysis of the cybersecurity risks. The question is, is it adequate that your mitigations for all risks is that you've reduced the risk to an

acceptable level for the whole system, or do you have to actually provide a justification for the mitigation of each and every single risk?

(Dr. Abiy Desta): Generally speaking, I believe we look at the system as a whole, not the individual risk. We would like to see that the risk for your medical device as a whole has been reduced.

Man: To an acceptable residual risk. Okay.

(Dr. Abiy Desta): That is correct.

Man: Very good.

(Dr. Abiy Desta): Again, with regards to cybersecurity.

Man: Right. Okay. What about password protection? When you include password protection, you provide security but you also reduce availability of the device. What is the thinking on that?

(Dr. Abiy Desta): Again, that is recommended based on the appropriateness for the use of your device. The agency recognizes that, in some applications that might be an appropriate approach; for others, it might not. It's one of the things we would like you to consider in your design.

Man: And we do. Thank you.

Coordinator: Thank you. I would just like to remind participants if you would like to ask a question, please press Star 1 on your phone and, when prompted, please record your name. Our next question is from (Praboo). Your line is open.

(Praboo): Thank you. I want to get some clarification on the applicability of the guidance in terms of the submitted products. Is it intended to apply for newly submitted products or what part or aspects of it apply to older products that are fielded?

(Dr. Abiy Desta): This guidance is for submissions that are coming in. If it's a modification to an existing product, it might or might not be appropriate to have included this depending on what generation it might be. I would advise you to talk to you the branch or division where your device is being reviewed to see what their expectations might be.

Man: Thank you.

Coordinator: Thank you. Our next question is from (John Aoki). Your line is open.

(John Aoki): Yes. My question deals with patient data. Is cybersecurity primarily important because of patient data or is it so that people can't hack into your system and ruin your system? I mean, is the main goal patient data?

(Dr. Abiy Desta): The main goal is device integrity and the function of the device. If patient data is part of that device integrity then the data is important and just as important is whether that device is providing diagnostic or therapeutic function. I'm not sure how to separate out one functionality from another. We would like the device to be as secure as possible regardless of what aspects are in there.

(John Aoki): If it is a standalone unit and it's not hooked up to the Internet but there is perhaps a USB port in your system so you can do physical updates to your system?

(Dr. Abiy Desta): Yes, I mean, that's a potential vulnerability where both the patient data and the functionality of the device can be compromised, so as part of your design of your device, that is a risk you should consider and mitigate for.

(John Aoki): If someone inserts just any type of USB drive maybe you can prohibit it or something like that? It has to have a certain pass code on the USB drive?

(Dr. Abiy Desta): Again, the idea of this guidance is not to be prescriptive as to the method. It is just one of the areas of risk that you would like the...

((Crosstalk)).

(John Aoki): All right. Thank you.

Coordinator: Thank you. Our next question is from (Mike Amote). Your line is open.

(Mike Amote): Yes, I have a two-part question. One is this is guidance and if somebody submits something and you determine whether they have not really followed the essence or the spirit of the guidance, exactly what does the FDA intend to do in that case? The other is how is the FDA actually going to make a determination that what has been submitted is actually adequate under the guidance?

(Dr. Abiy Desta): Again, this guidance is a recommendation. If we get a submission that we feel may or may not adequately address cybersecurity, we may have that discussion with the sponsor about how those risks may or may not require mitigation depending on the risks associated with the device. I think each branch will make a decision as to the safety of the device.

Coordinator: All right. Thank you. Our next question is from (Laurie Trotter). Your line is open.

(Laurie Trotter): Yes. Could you clarify if there is a mobile app that is intended to control a device? Does that fall under the scope of this guidance document?

(Dr. Abiy Desta): A mobile app that is intended to control a device is an accessory to a device so it would be a medical device, so there would need to be some considerations as to what risks might be present to that app.

(Laurie Trotter): Great. Thank you.

Coordinator: Next question is from (Mike Tusken). Your line is open.

(Mike Tusken): Hello. In the cybersecurity world, I'm thinking that there are two kinds of risks. Those that could impact the safety and effectiveness of the device. And there are other risks that could impact the financial or picture of the company -- loss in sales, penalties, fines, etcetera. When I read the guidance, I'm assuming that it is all focused on maintaining the device as safe and effective; is that correct?

(Dr. Abiy Desta): That is correct. Maintaining the safety and effectiveness of the device is within our regulatory authority so that is what it is focused on.

(Mike Tusken): And those other cybersecurity risks that could result in penalties would not be included in this guidance?

(Dr. Abiy Desta): Again, this guidance is focused on the regulatory authority of the FDA which is safety and effectiveness of medical devices.

(Mike Tusken): Thank you very much.

Coordinator: Thank you. Our next question is from (Paul Delarova). Your line is open.

(Paul Erota): I assume that's me. It's (Paul Erota), I'm with Covidien. You mentioned collaboration between the customer and the medical device manufacturer. This becomes a fairly complex proposition and I'm thinking in particular about the requirement for an authenticated user and how many devices today have service passwords that are widely available on the Internet.

It seems to me that this tends to drive those devices that use such passwords to be network connected in order to provide that kind of flexibility and user authentication because if the facility wishes to change the authentication for a particular device and, now, the manufacturer can no longer access it because the facility has changed it, how do you envision that getting reconciled?

(Dr. Abiy Desta): I recognize that there are difficulties in terms of providing easy access for maintenance and other functionalities in providing security. I'm not sure the agency would be prescriptive. The agency would like to have manufacturers consider the potential risks versus the benefits and be able to think about adequate methods of mitigating the risks while still providing the functionality and the access that might be needed to patch or maintain a medical device. I recognize my answer is not really an answer but it is also an attempt not to be prescriptive but to allow you to think creatively and come up with an answer.

Irene Aihie: We'll take the next question.

Coordinator: (Lance), I'm so sorry. You could repeat your question now.

(Lance Gray): Great. This is (Lance Gray) at Auditory. Between the draft guidance you guys sent out earlier in the year and the final, I noticed two differences. One was you had called out in the draft buckets -- confidentiality, integrity, and availability -- as if you kind of wanted us to bucket our risks into those buckets and, in the final, you did not really call that out. Are you expecting to see us do our risk analysis based on those types of buckets?

(Dr. Abiy Desta): The draft guidance was there not to be implemented but to get comments. The final guidance is what we would like to see being implemented. There were changes between the draft and the final guidance. Part of that was in response to the comments we received and part of that was to make sure that we were properly balancing our recommendations and the actual burden that might be presented to industry.

(Lance Gray): The second one which is not really related, it's just something new in this versus the draft was you actually say that the FDA does not need to review or approve software changes solely for cybersecurity as long as we describe that in our cybersecurity update patching plans. Can you expand on what that means? Does that mean we don't have to address cybersecurity when we do an update?

(Dr. Abiy Desta): What we're trying to say there is if you're doing an update that would not require a new submission, updates would be considered maintenance and routine updates where you're providing patches related to cybersecurity would not be something that would require additional premarket submission.

(Lance Gray): Just so I'm clear. If I do an update based on cybersecurity only, it doesn't require an update to the submission, but anything outside of cybersecurity, then that falls under other submission requirements?

(Dr. Abiy Desta): Again, this does not address other types of updates in terms of if you're providing a patch to your software system because of cybersecurity. That would be an area where the FDA would not require additional information. That statement was not meant to address other types of updates you might or might not do.

(Lance Gray): That's the way I read that. Thank you. That's all.

Coordinator: Thank you. Our next question is from (Christine Tex). Your line is open?

(Christine Tex): Hi. Yes. This is (Christine) from Seneca Diagnostics. I have two parts and I think one you've probably already covered.

My first question is in the details of where in the 510(k) submission should this cybersecurity reside? And then my second part of the question that I have is since it has not been provided in our previous 510(k) submissions, I would imagine we would have to baseline when we would submit our next special 510(k) for our respective device; is that correct?

(Dr. Abiy Desta): To your first point, this would be in your software risk analysis section. The cybersecurity risk analysis would be called out specifically but would be part of your software submission. In terms of your second question, could you repeat that? I'm not sure I fully grasped what you're asking.

(Christine Tex): Since we've never provided this information before in our 510(k) submissions, if I have an update that would require a special 510(k), we would actually have to essentially baseline all the requirements of this guidance at that point in time; is that correct? We'd have to submit. When we submit a special now, we submit based on any new information so, since we've never submitted this information before, we would have to submit it at that point in time?

(Dr. Abiy Desta): Yes.

(Christine Tex): Even though the change isn't necessarily related to cybersecurity?

(Dr. Abiy Desta): Yes. At least the cybersecurity section of your risk analysis would have to be complete.

(Christine Tex): Thank you.

Coordinator: Thank you. Our next question is from (Bob Caruso). Your line is open.

(Bob Caruso): Hi, this is (Bob Caruso) at Patel. Will the FDA establish a baseline set of controls based on device type, or would the set of security controls be established by an initial risk analysis that incorporate both the threat assessment and vulnerability assessment that is performed by the vendor?

(Dr. Abiy Desta): It would be by the vendor. The FDA would not be the one establishing the controls. The FDA would like to see justification for those controls and advocacy that they mitigate the risks in question.

(Bob Caruso): Would you foresee standard sets being developed over time for different classes of controls, say, a pacemaker, insulin pump, etcetera, that are unique to those particular devices?

(Seth Carmody): Hello, this is (Seth Carmody). I'm an expert at CDRA in the Offices of Vitro Diagnostics and Radiological Health. I would like to answer your question. I think that over time as we accumulate experience with the provided cybersecurity risk assessment that there is a repertoire that we identify with and look for in other submissions.

(Bob Caruso): Thank you.

Coordinator: Thank you. Our next question is from (Dan Smith). Your line is open.

(Dan Smith): Thank you. The FDA guidance emphasizes limiting user access and password strength requirements. If that responsibility is moved over to the help system through, as an example, active directory integration, is that considered a preferred solution essentially moving that responsibility to the help system rather that building it into the medical device solution?

(Dr. Abiy Desta): Again, that is a recommendation. If there are alternatives including moving it as you suggested that would mitigate the risks adequately, I think it would be one we would consider. I would not want to be prescriptive now and say that is something that you should do. Again, what we would like to see is threats posed by simple passwords or easy authentication be limited.

(Dan Smith): Thank you.

Coordinator: Our next question is from (Tina O'Brien). Your line is open.

(Tina O'Brien): Hi. I think you've answered this question previously but I'm in queue to ask it now. If we have a device, a low risk device from a cybersecurity perspective, that we categorically just excluded from any vulnerability, in our software section, is a simple rationale of our thought process adequate or do we need to carry that through into our risk management documentation to show how we considered it and what the risks are or what the risks aren't I suppose?

(Dr. Abiy Desta): As far as the rationale, we would like to see at least some kind of a matrix of each risk you considered pointing to mitigation so that we have a better

understanding of all the different types of risks that had been considered and how they are being mitigated.

(Tina O'Brien): Excellent. Thank you.

Coordinator: Thank you. Our next question is from (Ray Riddle). Your line is open.

(Ray Riddle): For a network controlled or connected medical device, when you are doing your assessment of the risks, how much can you rely on the inherent network security itself?

(Seth Carmody): This is (Seth Carmody) again. I think it's important to remember that you need to take into account that your medical devices could be going into a hostile environment. You may have no control over the security provided by the network which they're established. It would behoove you to adopt controls that defend your device singularly to defend it going into a hostile environment.

Coordinator: Thank you. Our next question is from (Joe). Your line is open.

(Joe): Yes. Relative to the mitigations that are being put in place, what considerations are you making around labeling changes versus actually design changes to the product to be able to mitigate some of those security vulnerabilities?

(Dr. Abiy Desta): I think where appropriate labeling could mitigate the vulnerability and it conveys to the end user how to mitigate those risks.

(Joe): Great. Second follow-up question. As I understood, this was applicable mostly to new products that are being submitted for 510(k)s to consider for 510(k)s --

products that are in the market already that are potentially just getting updates -- wouldn't be subject to it unless they are being refiled for a new 510(k) submission; is that correct?

(Dr. Abiy Desta): I'm not distinguishing just getting updates versus a new 510(k) submission but, if you have a product that is on the market that requires a 510(k) because of changes you've made, that would be up to the discretion of the review branch to see whether cybersecurity risks need to be concerned or whether the device, as it stands alone, poses low risk and the modification you propose could go through without addressing cybersecurity.

(Joe): But just to clarify. As companies are making priorities on new product adoption versus adopting a legacy product that may have been in the field and close to an end of life, how is the FDA seeing the relative risks of those differences and what standards or expectations are you putting in place for different device vendors?

(Dr. Abiy Desta): I'm not sure the agency is putting in the expectations. We would like to see all vendors consider cybersecurity risks when they design and produce a device. The FDA recognizes that, with legacy devices, these modifications may not be practical or feasible but we don't want to set expectations based on that.

(Joe): Great. Thank you very much.

Coordinator: Our next question is from (Yvonne Newell). Your line is open.

(Yvonne Newell): Hey. I have a question for the software package that it delivered through the Web side or cloud, how should we handle that cybersecurity issue?

(Dr. Abiy Desta): Could you repeat the question?

(Yvonne Newell): Like, software delivered through the Web site or through the cloud, how can we mitigation a risk analysis that would be an impact on the cybersecurity?

(Dr. Abiy Desta): You're saying you have a medical device that the wrong software got delivered through the cloud?

(Yvonne Newell): Yes. Or, like, a service package. Like small updating software. Software for the software updates through the Web site or through the cloud, how can that--

(Dr. Abiy Desta): If you are providing patches to software updates for clouds, the agency would like to see some kind built-in authentication so that the device where the patch is being placed trusts the course from which the patch is coming. In terms of standalone software, that might exist in the cloud or on the network someplace. I think there needs to be an analysis of the environment in which that software exists and what risks might be present to it.

(Yvonne Newell): So just a password would be good enough or what else additional information we should consider?

(Dr. Abiy Desta): Again, we don't want to be prescriptive. We would like you to choose a method and be able to justify why you feel that method is appropriate.

(Yvonne Newell): Thank you.

Coordinator: Next question. (Crystal), your line is open.

(Crystal): Hi. Which devices are subject to the cybersecurity? Is it mostly software? I know you mentioned you have to maintain the device integrity. I'm just not sure which devices would fall in cybersecurity.

(Dr. Abiy Desta): Medical devices that are vulnerable to cybersecurity risks will be subject to this. In the section that deals with integrity of the device, we were trying to specify from the time the device has been manufactured to the time it leaves your facility and goes to the vendor meaning the time that you have it, you should be able to have some documentation that assures that that device's integrity has not been compromised.

(Crystal): Would you be able to give an example of which devices would be subject to cybersecurity?

(Dr. Abiy Desta): Again, a device that is vulnerable to cybersecurity threats. If it has some kind of computer logic that could be reprogrammed, if it has software running on it, if it's the software that is an actual device, all those would be subject.

(Crystal): Do you have an example?

(Dr. Abiy Desta): For instance, a CT scanner with software that runs the different therapeutic modes that would be device that would be subject to this guidance. If you have a blood pressure cuff that transmits its information to a mobile app, it would be subject to this guidance.

(Crystal): I see. Yes. That does answer my question. Thank you.

Coordinator: Our next question is from (Frank Sutton). Your line is open.

(Frank Sutton): Hello. Yes. I hope this question will make sense to you. I'm looking here. What can we expect as the disposition of the FDA for submissions coming forward? Is there a leeway period? Development finished six, seven, twenty years ago, something like that, we're just getting around to it -- I'm not saying

that's actually the case; I'm just giving you an extreme -- can we expect a leeway disposition from the FDA moving forward for submissions?

(Dr. Abiy Desta): I think when you provide a submission; we would like to have a conversation with you about cybersecurity. Whether it is appropriate to provide the leeway or not, I think will be made by the review branch.

(Frank Sutton): So your answer, if I may rephrase it and you can correct me, is on a case-by-case basis we'll see moving forward but circumstances will be taken into consideration?

(Dr. Abiy Desta): Yes.

(Frank Sutton): Thank you very much.

Coordinator: Our next question is from (Phillip Lee). Your line is open.

(Phillip Novalee): Thank you. (Phillip Novalee) from (Grafulstead) Elastic Solutions.

My question pertains to labeling or instructions for use. If there are any best practices that you could provide as far as the scope or what aspects of cybersecurity other than what was mentioned -- firewall or antivirus software -- that should be captured in our instructions for use?

The second aspect of my question pertains to the risk management guidance. Can we use the standard ISO-14971 in lieu of an IT network specific standard on risk management?

(Dr. Abiy Desta): To your first question, I'm not sure if the agency could provide specific examples. It depends on the use environment of your device that you would

need to provide us with labeling. If you have an idea of where your device might be used or if it's a home-use device, you might want to provide labeling instructions to a home user as to what the minimum configurations should be based on the security that you've implemented in your device. If your device is going to a hospital, clearly, the labeling might be different. It will really depend on the use environment of your device. And I'll defer to one of my colleagues to answer your second question.

Linda Ricci: This is Linda Ricci. I'm also from the Office of Device Evaluation. Can you repeat the second half of your question, please?

(Phillip Novalee): Basically, if we could adopt the ISO-14971 risk management in lieu of using an IT network specific standard on risk management?

Linda Ricci: Certainly, the ISO-14971 standard is an FDA recognized standard for risk management and you are certainly welcome to use that as part of your risk management process. It is also important to understand that the risks that you might be trying to identify with regards to cybersecurity might also be well characterized by other standards that deal more with IT security. And so, if you wanted to use a combination of the two that would certainly be an option that we would be open to.

(Phillip Novalee): Thank you.

Coordinator: Our next question is from (Jordan). Your line is open.

(Jordan Latog): Hi. Yes. (Jordan Latog) here. If we were submitting a 513(g) application for information and from past applications we are seeking to be a non-medical device but it is used in the medical field and pass a similar type data, is there

anything we need to elaborate more on cybersecurity than we have in the past?

(Dr. Abiy Desta): In the 513(g)?

(Jordan Latog): Yes.

(Dr. Abiy Desta): A 513(g) would not be a submission where the agency expects to see cybersecurity information.

(Jordan Latog): Would it be helpful?

(Dr. Abiy Desta): A 513(g) is a Request for Information about the classification of the device. It will not be a safety and effectiveness review assessment. It would not be necessary to do that there.

(Jordan Latog): All right. Thanks.

Coordinator: Our next question is from (Dario). Your line is open.

(Ron): Thank you. Hello. It's (Ron) and (Dario). I would like to ask another question about updates to the software. I see two aspects of the updates. One of the aspects you covered recently about the security of the updated itself so that we can mitigate the risks of invalid update or a failed update. However, another question I have is in case our update includes new features for the application or changes in the behavior of our application, how should we decide if this is allowed by the FDA to be under the same submission of the whole application, or if this update has to be separately submitted? What is the criteria here?

(Dr. Abiy Desta): If your update is changing the specification of how your device functions, then that would be a modification that would probably require a new submission. If your update is only patching cybersecurity vulnerability and not affecting the specification for which your device has been cleared, then that would not require a premarket submission.

(Ron): When we define a specification of how the device is functioning, does it include a new feature our user might get with an update which was not clearly defined when we did the submission, however, it just adds another ability for the user, for example, to review the data or to somehow work with the data that it gathers with the device.

Is there a possibility to add such a feature without violating our previous submission?

Linda Ricci: Your question, really, is outside the scope of the cybersecurity guidance. I mean, the cybersecurity guidance is talking about updates that are specific to cybersecurity vulnerabilities that you're trying to patch.

If you're asking a question about when to submit a new 510(k) for changes that you're making to your device whether it be software or otherwise, I encourage you to check our Web site. There is a document called "When to submit a new 510(k)" that will cover when you change the functionality of your device, software or otherwise, what would require a new 510(k).

And, if you have further questions regarding that, I would encourage you to contact the review division that handles your types of devices to have a more specific conversation.

(Ron): All right. Thank you. I understand.

Coordinator: Our next question is from (Claudia Jackson). Your line is open.

(Claudia Jackson): Yes. Hi. I have a question surround the information, I'm sorry, the security that you would submit to the FDA.

For each submission that you do, you do a submission for a significant change in your device. Because your device may have a legacy model or version, cybersecurity or the system of the cybersecurity around that device has already been established. A risk has already been mitigated and discussed.

But if I do a modification or I do a significant change to that device that has nothing to do with the cybersecurity of that device, my submission still has to include -- this is the question -- still has to include the risk analysis that was done maybe two or three models or versions ago? That's the question. I hope that was understandable.

(Dr. Abiy Desta): If you feel that the risk analysis that was done two or three years ago adequately mitigates risks that are of present time, you could reference that risk analysis.

(Claudia Jackson): But I would have to submit that risk analysis in its entirety? It would be based up on test cases and have a different traceability matrix so I could get kind of lost in what the FDA is looking for.

Linda Ricci: Yes. You present a very challenging situation in which you've actually some work on cybersecurity for legacy devices that was not presented previously to the FDA and, now, your versions have moved onward so the rationale and the risk analysis for what you had done previously, the notes still apply, if you can't map directly into your submission now? Is that a summary?

(Claudia Jackson): Right. Thank you.

Linda Ricci: Certainly, we want to evaluate -- evaluate is kind of a strong word here -- but we want to have known that you evaluated the cybersecurity risks for your device. So, in those cases, certainly, I would talk to the review division and make sure you have an open dialogue with them explaining what you have done previously. But at least, at a minimum, I think you could provide a summary of the risk mitigations that you put in place to address cybersecurity, reference where they were done and the lifecycle of your device and how they still apply.

(Claudia Jackson): That's reasonable. Thank you.

Coordinator: Our next question is from (Paul Singh). Your line is open.

(Prestal): Hi. My name is (Prestal) from BioRite Solution. My question is in regards to mitigate the risks arising from cyber threats, is there a guidance or minimum standard that is recommended during the validation testing, or is there anything coming up?

(Dr. Abiy Desta): At this time, there is no guidance that the FDA has issued on that topic. The FDA has recognized a number of standards on this topic, but also, if you believe that you have adequately met that threshold and you could justify that threshold to us, that would be something we would consider.

(Prestal): Thank you.

Coordinator: Our next question is from (Michael Seeberger). Your line is open.

(Michael Seeberger): I have a question regarding the deliverable where it talks about the companies have a summary or a plan for proving validated software updates and patches.

Since a lot of medical devices contain third party software such as a device driver or operating systems, are you expecting that the documentation should include risks or vulnerabilities and mitigations/controls or monitoring, say, operating system vulnerabilities that aren't directly responsible of the manufacturer and to have a plan for controlling those or for updating patches?

Also, when you mentioned the summary of a plan, I'm curious how much detail the FDA expects in the submission or is a summary basically that the company will monitor, say, an OS vendor's security patches and make appropriate plans when a critical issue comes up to field a patch? Is a summary enough, or is more detail expected?

(Dr. Abiy Desta): We would like to know how you are approaching that issue to some detail. We don't want exact timelines of what and how often but, if you have a third-party software, how you are approaching cybersecurity. Are you locking it down so no updates are possible? Are you providing your customer with means? Are you expecting your customers to be the ones that are doing that? We would like to have some idea of how you are approaching this issue.

(Michael Seeberger): That makes sense. Thanks.

Coordinator: (Dina Castle), your line is open.

(Dina Castle): Hi, my name is (Dina Castle) from (Unintelligible) in Miami. I have two questions. The first one is the manufacturer responsible for the cybersecurity risk induced to the medical instrument by the hospital network and if you have

any recommendation or guidance? The second question is how do you recommend handling the probability of occurrence of a cybersecurity risk when it is part of the system and we need to estimate the probability of the hospital situation? Thank you.

(Seth Carmody): This is (Seth Carmody) again. Could you repeat the second part of your question, please? The second part.

(Dina Castle): The second question is how do you recommend to handle the probability of occurrence of a cybersecurity risk when that risk is part of the system and we need to estimate the system probability of we have those situations that can be their reporting to repetition or delay of results reported to repetition?

(Seth Carmody): It's going to depend. Device manufacturers will be the experts in how their device acts. You need to be controlling for risks that come along with being as a network system. You should assess risks just like you assess risks due to what other type systems are on your analyzer and control them for delaying results are low risk results due to a hack. So, yes, you should not rely on the network. These systems are going into hostile environments. You already are experts in assessing risks of that type of system. What would happen if you had to delay in result or erroneous result whether it's to an app solution or sample volume issue or somebody intentionally trying to cause harm?

Coordinator: Our next question is from (Matt Shaw). Your line is open.

(Matt Shaw): Yes. My question is around how will the enforcement be for this? I know that there will be questions asked during the 510(k) submission process and just the appearance of it, but also, will this now become part of the standard Q-fit inspection? I'm just curious what the enforcement for this will look like.

(Dr. Abiy Desta): Again, this is a premarket guidance. It does not deal with post market or enforcement issues.

(Matt Shaw): All right. Great. Thanks. Appreciate it.

Coordinator: Thank you. Next question is from (Laurie Trotter). Your line is open.

(Laurie Trotter): Hi. I had a question regarding the scope and the inclusion of programmable logic. Can you provide some guidance around that including what your definition of programmable logic is?

(Seth Carmody): I would interpret programmable logic as a hardware functionality that can be reprogrammed. There are plenty of resources that currently exist in other sectors that you can look to in terms of guidance. We have no specific guidance on those technical items but I'll point you to government agencies such as (Mist) or other sectors such as banking or industrial control systems or defense sectors.

(Laurie Trotter): Thank you very much.

Irene Aihie: Next question, Operator?

Coordinator: I'm sorry. Are you able to hear me?

Irene Aihie: Yes, we can hear you now?

Coordinator: (Diane), your line is open. All right. We're going to move on. (John) with ZIMA Medical. Your line is open.

(John): Hi. I have a question about the encryption of data communications between medical devices and some external devices.

Since the manufacturer is not required to follow any kind of industry standards and we can choose whatever encryption scheme that we think is suitable, is there a basic minimum requirement about the strength of encryption that is needed, like, from a mathematical analysis standpoint?

Is there any minimum requirement that it has to meet to be able to prove the encryption scheme is strong enough to withstand hacker attacks?

(Dr. Abiy Desta): I think the agency's perspective is for you to provide a rationale for whatever scheme that you've chosen and whatever strength it is that is adequate to mitigate the risks your device faces in the use environment. The agency is not going to be prescriptive on that.

(John): Thank you.

Coordinator: Thank you. Our next question is from (Deborah). Your line is open.

(Deborah): Hello. I have two questions. The first is for submissions that are currently under review, is there something that you anticipate that it would be brought up during the review process if we've already received our first response from the FDA?

(Dr. Abiy Desta): If the submission was submitted on October 1 or later, depending on your device type, you may or may not.

(Deborah): And then the other question is under the guidance there is a section that goes into the different means to limit access to trusted users only. Would it be

possible to, for example, the bullet says "When the accuracy device is to be authentication of user, for example, user ID and password, smart card, biometrics," would you be able to provide an example where that would be most appropriate?

(Dr. Abiy Desta): To provide an example, it could depend on what your device is and the use environment. There might be a use environment where providing such authentication would not be practical so if your device is being used in a surgical suite, that would probably not be an appropriate method of authentication. In other use environments it might.

What the agency would like to see is for you to consider different methods and choose the one most appropriate for your use environment that reduces the risk access.

(Deborah): Yes. This may be something that we may put in as a general comment to the guidance. It would be helpful if there were examples, I mean, obviously, we don't expect the FDA to give us a recipe book but if we could gauge better where the FDA's position is and maybe somebody could cite some examples that would be helpful.

(Dr. Abiy Desta): Thank you.

(Deborah): Thank you.

Coordinator: Thank you. Our next question is from (Debbie Brown). Your line is open.

(Debbie Brown): Hi. This is (Debbie Brown). There was a question somewhat like this earlier but I think this is slightly different. Are the cybersecurity guidelines applicable to mobile apps that are subject to enforcement discretion?

(Dr. Abiy Desta): Mobile apps that are subject to enforcement discretion are except from the FD&C act so there will be no submission required so there will be no submission that the FDA would be reviewing. At the same time, just as a general factor, we would encourage you to consider cybersecurity as part of your risk assessment regardless of whether the FDA will see that submission or not.

(Debbie Brown): Thank you.

Coordinator: Thank you. Our next question is from (Sanjay). Your line is open.

(Sanjay): Yes. Thank you for the platform. We just have a question in terms of the cybersecurity, how much it extends with regards to the cybersecurity within the medical device application or also to the interfaces to the third party tools that our device would interface on and also with? Do we have to have requirements for the third party tools for the cybersecurity?

(Dr. Abiy Desta): In your submission, are you describing the risks associated with third party tools also, or is your submission going to be limited to your device?

(Sanjay): We would have the third party tools -- we would have the risks identified for those tools as well. But then, obviously, we don't develop those tools so we don't have a handle in terms of how they manage their cybersecurity environment.

(Dr. Abiy Desta): Yes. While you don't have a handle on how they manage their cybersecurity environment, it would be useful to know that you have considered what risks might be posed to your device from being in that environment and trying to address any risks that might be present because of that.

(Sanjay): Thank you.

Coordinator: Thank you. Our next question is from (Edward). Your line is open.

(Ed Thomas): Hi. This is (Ed Thomas) with Life Science. I've actually got three questions but I'm going to ask two, though, in the interest of time.

The first one is for some of the software including Primeware and Beta software, the cybersecurity mitigations for the risk management are inherent to the fact that the software is isolated and it would not be accessed from outside and there would be no ways of communicating with the software. There are no particular software mitigations built into the software necessarily. I'm interested to know if, with this new guidance, you are specifically looking for further software mitigations for cybersecurity or not? I guess I'll do them one at a time. That was my first question.

(Seth Carmody): Just for clarification you are referring to a device which would require physical access?

(Ed Thomas): Correct. Let's say you've got an isolated chip inside of a device which, in order for corruption of the software, one would need to crack open the device and access the chip.

(Seth Carmody): I guess there are still risks that you've identified and somebody would have to view that, so I mean, discussing what the risk associated with it is and to acceptable risk level indicates that. And then, therefore, you wouldn't have to control for it.

(Ed Thomas): My second question is around on the slide you did mention protecting critical functions when cybersecurity is compromised. There were examples of drivers. Do we have a better idea of what those critical functions are or are that something that; basically, we define at the design level? Are you expecting that to be documented specifically or does that just go along with other critical to safety requirements? I'm not sure what that definition entails.

(Dr. Abiy Desta): Again, I think that would depend on your device. I think the thinking by the agency there if there are functions that your device has that is life-sustaining, it would be important to try to make sure that those functionalities are maintained regardless of failures on other components of your device.

(Ed Thomas): Do you see this playing with the safety classification of that device, or no? Interacting in a way?

(Dr. Abiy Desta): No. We are not saying if you're this class or this class you have to approach this. I think our recommendation is that, for your device, you look at all the risks involved and, if there are risks that are so high that there should be some kind of mitigation put in place to prevent it from failing when other parts fail, that you consider that.

(Ed Thomas): Thank you.

Coordinator: Thank you. Our next question is from (Emmett). Your line is open.

(Marmot Thomas): Hello. This is (Marmot Thomas). I had a question related to the submission. In the submission, do you expect to get the details of the residue of vulnerability and, if you expect to receive that, to what detail do you expect them?

(Dr. Abiy Desta): You mean whether you have risk after you've mitigated for the device?

(Marmot Thomas): Well, residual vulnerability, the technical details of those risks. Do you expect to receive them?

(Dr. Abiy Desta): I think a general overview of what those are would be adequate. I don't think we need an in-depth technical detail.

(Marmot Thomas): Excellent. Thank you very much.

Coordinator: Thank you. Our next question is from (Ian Nimerov). Your line is open.

(Ian Nimerov): Hi. With the interesting cybersecurity, has the FDA changed the way it is looking at open source software that is built into products?

(Dr. Abiy Desta): No. The agency has not changed how it reviews software in general, open source or otherwise.

(Ian Nimerov): Thank you.

Coordinator: Thank you. Our next question is from (Mike Mensinger). Your line is open.

(Mike Mensinger): Hello. My question relates to validation of security patches. You mentioned that upon patching a system you expect the plan to include validation of the functionality so it works properly. My question relates to some new platforms that are coming out on the cloud where platform updates are not under the control of the device vendor; that the updates are automatically rolled out. In this particular instance, do you have any guidance on how medical device vendors should deal with that?

(Dr. Abiy Desta): Not in this instance. I will just say that would not be just a cybersecurity issue. That would be a larger software update issue.

(Mike Mensinger): If we had a plan where we could detect that the update is being rolled out and does a validation at that event, is that something that you had considered acceptable in the past?

(Dr. Abiy Desta): Let's say you have something on an Android platform and Android platforms are continuously being updated, the assumption is that, before providing a patch to your medical device that is on there, you would have made sure that it will work with whatever new version may be coming or has been implemented since your last update. I'm not sure if that answers your question directly.

(Mike Mensinger): Sure. That makes sense. So, if there is a breaking change from a platform, as long as the device vendor provides the change that the user can install to make it compatible that would be acceptable?

(Dr. Abiy Desta): Yes. But, again, I think that become a larger issue than just cybersecurity.

(Mike Mensinger): Sure. Thank you.

Coordinator: Thank you. Our next question is from (Jason Yome). Your line is open.

(Jason Yome): Hi. (Jason Yome) from (Unintelligible). The question is regarding the custom firmware that was developed in-house. Does the risk analysis that is getting filed as part of 510(k) should include a risk analysis for the firmware cybersecurity risks? We already planned for the OS and the workstation software but I don't think we have any plans for the firmware part.

(Seth Carmody): This is (Seth Carmody) again. I think that you should consider cybersecurity risks in regards to your firmware.

(Jason Yome): Thank you.

Coordinator: Thank you. Our next question is from (Dan Schmidt). Your line is open. (Dan), you may have your phone on mute? All right. We're going to move to the next question. (Elizabeth George). Your line is open.

(Elizabeth George): Yes. This is (Elizabeth George) with Phillip Cattier.

The question I have is a number of times you've mentioned reliance on the reviewers during the 510(k) process. I know the reviewers have a standard training program. I'm just curious as to where they stand in being trained in understanding what a cybersecurity risk is, what vulnerabilities are, and even what some of the nomenclature that the vendors will be submitting in the submissions?

(Dr. Abiy Desta): We continue to provide reviewers training and we also continue to have subject matter experts ready for those reviews to rely on so when the submission comes if there is something they are unfamiliar with.

(Elizabeth George): Thank you. Appreciate that.

Coordinator: Thank you. Our next question is from (Gretel). Your line is open.

(Gretel): Hello, this is (Gretel) from (Unintelligible). My question has to do around with the how is this going to address the refusal to accept policy in light of this new guidance? There have just been a lot of recommendations to make determinations with reviewers as to whether or not we need to include the

security. My concern is that, with the refusal to accept policy, we could get the submission kicked out even though we have agreements with the agency already to not include security for whatever reason.

(Dr. Abiy Desta): That would not apply here so your submission would not be kicked out because of this.

(Gretel): I just wanted to clarify that because we hear a lot about that. Thank you.

Coordinator: Thank you. Our next question is from (Steven Garsky). Your line is open.

(Steven Garsky): Hi. One of the things that happens when driving down residual risks of cybersecurity is it becomes evident that the residual risks lie in the hands of the responsible organization and there is a balance between usability and authentication as you know. Some of those hazards just don't go away as a result or they can only be driven to a certain level because of reliance on the responsible organization to do their job as prescribed in the labeling for the use of that particular device. What is the agency's thinking on what the appropriate handoff is for the responsible organization? Because you can only mitigate so far in some cases. Thank you.

(Dr. Abiy Desta): The agency recognizes that so one of the ways to ensure appropriate handoff is to provide it in your labeling as to what your device is or what risks your device is mitigating against and what y our expectation is in the use environment. The FDA would like to see better communication between, I guess, vendors and users about how to manage your risks as a whole.

(Steven Garsky): Thank you.

Coordinator: Thank you. Our next question is from (Gary) with Welch Allyn. Your line is open.

(Gary): Hi, this is (Gary) with Welch Allyn. We had a recent submission and the FDA came back with the question of cybersecurity requirements because our requirements are hard to find. What are you actually looking for because of the cybersecurity requirements?

(Dr. Abiy Desta): I'm not sure I could speak to specific submissions. I would say that the agency may ask you questions regarding as to how you've mitigated risks that are associated with your device and the expectation is that you could provide information and justification for approaches that you've taken.

But I would further encourage you to talk to either the reviewer or the grant chief of the device being reviewed.

(Gary): Thank you.

Coordinator: Thank you. Our next question is from (Shelby). Your line is open.

(Shelby): Hi. I'm (Shelby) from Stryker. I would like to ask, if my device has Wi-Fi capabilities but it is not in the public network, does it still require cybersecurity?

(Dr. Abiy Desta): If your device is vulnerable because it is connecting to a network by which it can be compromised, then that is a risk that we would like you to consider and provide information for us of how you considered that risk and mitigated against it.

(Shelby): Thank you. I have just one more question. (Unintelligible) to qualify?

(Dr. Abiy Desta): It depends whether the mobile app that you are referring to is a medical device that is being regulated or is a medical device that has been under enforcement discretion by guidance. It depends.

(Shelby): Perfect. Thank you so much.

Coordinator: Thank you. Our next question is from (Claudia Jackson). Your line is open.

(Claudia Jackson): Yes. I have a question about the healthcare IT framework. Because of the medical device manufacturer that I work for, we fall under ONT regulations and HHS regulations and CMS regulations as well as FDA regulations.

And so, some of the cybersecurity measures that we have taken we've taken for other agencies regulations and, with the FDA's guidance, is it going to remain in line with what was proposed as the health IT framework of all of these organizations? And just remain risk-based. That is my question.

(Dr. Abiy Desta): Yes. I appreciate your question. Unfortunately, I mean, I came prepared in terms of talking about this guidance and the policy implications, but that is larger question that I'm not able to answer.

(Claudia Jackson): Oh. Is there anyone on the panel that would be able to answer that question? It's about the guidance. Is the guidance going to remain within that health IT framework?

(Dr. Abiy Desta): The guidance will be applicable to submissions whether it's in the larger framework or not. If you are submitting to the FDA for a premarket clearance, the guidance will apply. However, the agency's guidance, I think, interplays

with ONC or what other Federal agencies may require, I don't think here, at the table, we are prepared to answer that question. I'm sorry?

(Claudia Jackson): Even though the FDA is heading up the health IT framework?

(Dr. Abiy Desta): I would suggest contacting the contact person for the health IT framework and maybe directing that question there.

(Claudia Jackson): Thank you.

Coordinator: Thank you. Our next question is from (Frank Sutton). Your line is open.

(Frank Sutton): Hello again. Yes. Nice to talk to you. A while back now, you answered a question saying where does the documentation go? -- The documentation that you ask for in the guidance document -- and you pointed to the risk analysis in the software. I don't disagree with you but I would like you to elaborate on your point because your general principles of software validation in the final guidance for industry and FDA staff talks to security measures as going into the software design specification and not the risk analysis. So could you elaborate and say where you expect our documentation to be present in our submission? Does that question make sense?

Linda Ricci: Sorry. I was having trouble with the microphone. This is Linda Ricci again. Certainly, there are many different sections of the software documentation in a submission that could characterize the risks and mitigations posed by cybersecurity as well as other things. We had pointed to the risk analysis in discussion for the cybersecurity more as a starting point.

Certainly, anything that is in your risk analysis that then points to mitigation, we would look for in other places that is common in addressing risks.

I don't think it's inconsistent when we were discussing with regard to this guidance that we expect you to start with the risk mitigation because, as has been stated previously, we expect this to be done in a risk approach.

Certainly, there will be other aspects of your design and implementation that may contain information related to the mitigation for your cybersecurity as with many other functions in your device.

I hope that answers your question.

(Frank Sutton): Yes, ma'am. If I may rephrase your answer just for clarity, you expect that risks go with risks that requirements go with requirements, and bugs go with bugs in our submissions?

Linda Ricci: Absolutely.

(Frank Sutton): Thank you very much.

Coordinator: Thank you. Our final question is from (Praboo). Your line is open.

(Praboo): Hi. One of the differences between the draft guidance and the final guidance is the mention of the core functions of IPDRR, the Identify Protect Detect Respond and Recover. Is there any expectation on the representation of IPDRR in the risk assessment itself for cybersecurity? Are there any expectations on how it is mentioned or handled so it is clear on how we're framing the risk assessment?

(Dr. Abiy Desta): I think that was meant to provide a general recommendations approach. I think your submission should follow the general format of software

submissions where you generally identify, as previously discussed, the risks accordingly, the designs accordingly, and so on.

(Praboo): So you're viewing it as more of a process framework to consider along the risk management cycle as we evaluate cybersecurity, but if we focus on, say, confidentiality and the clinical security of the device, that is really what you're looking for?

(Dr. Abiy Desta): I would say that is correct.

(Praboo): Thank you.

Coordinator: All right. There are no other questions in the queue at this time.

Irene Aihie: Thank you. This is Irene Aihie. We appreciate your participation and thoughtful questions.

Today's presentation, along with the slide presentation and transcript, will be available at www.FDA.gov/CDRAWebinar by Friday, November 7, under the tab "past Webinars and stakeholder calls 2014."

If you have additional questions about this guidance, please use the contact information provided at the end of the slide presentation.

As always, we appreciate your feedback. Again, thank you for your participation and this concludes today's Webinar.

Coordinator: Thank you. This concludes today's conference. Participants, you may disconnect at this time.

END