**Episode #3 Transcript – Bold Type Team**

00:00:10

Michael: Welcome to the Health Connective Show. I'm your host, Michael Roberts, and I've got a number of folks on today to talk about some critical factors that startups don't tend to think about in the medical device and digital health space. We've got people from two different companies here today. I pulled in Justin Bantuelle, the chief technology officer and chief operations officer for Health Connective. And we've also got some folks from Bold Type here as well. Jose, can you introduce yourself and your company? And then we'll go around the room and say hello to everybody. Sure.

00:00:37

Jose: I'm Jose Bohorquez, president at Bold Type. So we're a product development firm that specializes in connected wireless medical devices and digital health apps.

00:00:46

Michael: Awesome, guys. You want to say hello as well?

00:00:48

Mohammed: Mohammed, the chief software architecture and am Andres Echevarria. I am the chief operating officer at both. Awesome.

00:00:54

Michael: Thank you guys. Got so much brainpower packed into this one. One call here. So I'm very excited about that. Startups. And they've got so much to juggle as they get going. There's so many different things. Jose, you and I met a few years ago at a med tech conference, and I feel like everybody that got up in front of the up to the podium said, you need to think about this as soon as you start your company. And it was like every talk that we that came up, they all said pretty much the same. This is the most one of the most important things. You've got to keep this in mind right from the top.

So when we were talking about Jose and I were talking about potential topics that we could talk about today, he listed out three different items. We may or may not get through all of those three items today, but we'll give it a shot. But those three were cybersecurity, usability, and setting up your software architecture in such a way that it's not all part of the medical device. Obviously, like everybody knows, security is important, right? That's one of those key words that we think about, man, I want to make sure my phone's secure, my devices are secure. All of that kind of stuff. Theoretically we all get that. Yeah. That's important. We should do that. But what are the specifics that startups aren't really thinking

about? If they have some sort of device that has some kind of software, like so security aspects that we need to think about for startups.

00:02:05

Jose: At a very high level, the key is that a lot of medical device companies are not thinking about cybersecurity early enough in the process, and they don't recognize or they don't realize that FDA has become has just increased their focus. The cybersecurity file and documentation that comes in with the 510 application. And so it used to be that it was maybe it was not even required. And then it moved to being what seemed like an ancillary kind of last minute thing. And now FDA is saying, hey, listen, if there's potential risks to the patient, we want to see a cybersecurity file that takes this seriously. So you're getting companies submitting their 510 applications and having them completely rejected because they either don't have a cybersecurity file included or it's not adequate. So that's at the very high level.

00:02:49

Michael: Now people are getting rejected. Mean I get it. If you didn't have the plan, okay, shame on you for not having it. But people are trying and not including enough. Is that what's happening March.

00:03:00

Mohammed: Of this year. And so this is very new. The FDA actually literally put out guidance on this, saying that they have now the right of refusal of your entire application. If they don't feel your cybersecurity approach and that is your plan, your document, etcetera, is adequate. So in other words, they can actually do a cybersecurity review of your application and not go any further. They can just simply reject your rejected outright and say, go back and figure this stuff out before you submit.

Again, they put this to the forefront now, and this is, as I said, very new. It was a march, just march of 2023 without this guidance. That's put the industry sort of on notice that the FDA is taking a very critical eye towards this and really the focus of the cybersecurity, if you want to get into more details from FDA's perspective, is what they said is it's really all about harm to the patient and their focus. And so this sort of falls very much into our wheelhouse is on connected medical devices. So they're less critical of in fact, in their guidance there's criteria on where they apply these rules if you're unconnected. So you're a completely standalone device.

They take the view that the threats are significantly less. In that case mean somebody would have to physically walk up to it, presumably tamper with it, which could happen. But that's not their primary focus. Their primary focus is very much devices that are connected to the internet. So you can imagine very simply a device where a patient's it could be a device administering medication, it could be a device that's monitoring vital signs and vital data. And if an attacker could launch an attack from externally from the internet and hit all patients that have these device devices, they could knock them all out in one go. And that is what is concerning to the FDA, is that could your device be vulnerable to an attack on a large

scale through the through the internet? And then you start thinking from there? Well, what does that mean?

Ultimately, there's a desire. There's a desire to have devices, medical devices, for instance, be updatable, remote. And we've all gotten used to this. Idea of our consumer devices being remotely updated with features and capabilities, bug fixes, etcetera. So it's a it's a temptation to try to do that as well with medical devices. But oftentimes update systems are not well scrutinized. They're specifically for security.

So they're they work they're used in development. But people don't think of them as necessarily attack vectors, but they very much can be. So that's a simple example of one, which is sort of a backdoor mechanism where somebody doesn't necessarily have to attack the device. If you actually think about this. And when we treat cybersecurity, we treat this holistically. It's not just the device, it's the entire ecosystem that this device sits in. And so you can imagine a medical device and it could be the boundary of the medical device, could be just a small physical device. However, that device connects through the internet to an update server sitting in the cloud. Well, you don't have to attack the actual device. You could attack the update server, you attack the update server, and through the update server, you now have access to the device.

So they're not going to look at it and say, okay, well, what we care about is your device. They're going to look at the entire system and say, how do we make sure that the integrity of the device is maintained under conditions? So that's where you start getting into the more details. And so again, to what Jose said, and this is true of security in general in all systems. Right. If you think about this, security has to be something you think of. They want you've got to begin. We begin with the security architecture. What is that? It is a it is part of the architecture of the system. So if you try to apply security after the fact, it's very challenging. And if it can even be done successfully at all, because you, you may have already put things in place that are not easy to secure without massive change. And oftentimes you're not willing to do that. So if you build security from day one, if you think of the necessary security from day one, you actually end up with a much more efficient and much more appropriate security system than trying to come at it.

00:07:06

Michael: So has Bold Type been in the position where you have to advise somebody, you're too late to the security game, and you're going to need to do some major overhaul to make it work?

00:07:16

Jose: Typically, clients are coming to us early in the process to do the product development for them. And so of course, we're thinking of those things quite early. I mean, we can think I can think of maybe one client off the top of my head that had some very significant vulnerabilities. They already had a product on the market and came to us. And when we looked at it, I mean, we we're just kind of shaking their heads like, you're just going to have to rewrite this entire application, because on the one hand, they had pretty dramatic security vulnerabilities.

Secondly, they had practically no documentation on the system. And with FDA, when you're doing software development for FDA, it's not just the development, it's the documentation of the system. And people kind of tend to think, oh, I'll write the software and then I'll do the documentation. That's not it doesn't work right. FDA is looking for you to have followed a process. So it's very challenging to kind of go back in time and put together a plan and risk analyses and requirements and all of that. If you didn't do it at the outset.

So for most of our clients, it's not an issue because we're doing the development for them. Sometimes people come to us with an older legacy type of product, and we look at it and we're like, yeah, you're pretty much going to have to start over. I mean, you can take some of the concepts of what was done in the original system. But Mohammed was saying, if the foundation, if the architecture is right off the bat full of vulnerabilities, there's not much you can do about that.

00:08:33

Mohammed: Just add to that. And there's another facet which I just like to offer with regards specifically to cybersecurity, that isn't true of the rest of the risk based development that we do for FDA, which is as part of your cybersecurity, already recognizes that cybersecurity is an ongoing threat. So you may analyze your system, put in place all the controls needed to submit a secure system today. But that's not enough. FDA will then turn around and say, okay, how do you maintain that posture? How do you ensure that your device remains secure six months after release, eight, 12 months, etcetera? So you need to propose to them a plan on how you will achieve that.

Now, I haven't seen this yet, but it'll be interesting to see if FDA does follow through with all this. Is will they actually come back two years down the road after they've approved the device? And so I'm not aware of anyone that's gone through this. It's possible that it's happened, but would FDA actually come in and ding you two years after the fact because you hadn't followed the plan that you proposed? And perhaps there is a vulnerability now that you have not closed, could they pull your product off the market for that reason? They've done it for other safety reasons, but I'm not aware of them doing it for cybersecurity reasons.

But I'm not saying it's not going to happen. There is a possibility that, well, with the emphasis that they're put in. So it's not enough just to design your product they want and submit it. You have to be serious about maintaining that level of security for the life of the product, which is a commitment that again, yeah. Do people plan? Do companies plan for that they want? It's not just about launching a product. It's about how do you keep that product in the market? A lot of what.

00:10:16

Justin: You're saying about that maintenance reminds me of kind of the process that you often have to go through for soc2 compliance. I'm curious how you feel like something like that enters into the equation and how much that covers you versus considerations. Beyond that, there's.

00:10:30

Mohammed: A good deal of overlap with in security spaces in general, again, where FDA is focused. And there's some subtleties here. FDA's focus is very much on harm to patient. It's interesting question, because we oftentimes look beyond just harm to patient because we consider that our clients may get harmed. And so there's harm to business as well reputation etcetera, which can occur. You decide the security. And so we look at that sort of vector as well. But from FDA's perspective their sole focus is harm to patient. Now what does harm to patient really mean? That harm to patient is not just there's the obvious harm to patient. If you're dispensing medication or doing something, you shock the patient or you electrically hurt.

You can you can actually hurt them physically. But there's also harm to patients due to misdiagnosis. There's harm to patient, for instance. I mean, think of a very simple example. In a large scale system, you your system has some vulnerability where it gets attacked and data from one patient ends up being associated with another patient. Now that could very well lead to misdiagnosis of the patients, because you're just looking at the wrong data and lead to harm to patients that way. So there are other vectors of harm that can occur that are nontraditional in the security world. It doesn't mean that your information was necessarily stolen. It doesn't mean that your information. It doesn't mean that it was a denial of service where you stopped working. Although those are also threats. It could be enough things that are innocuous in other systems but cause harm to the patient. In this case, there are some special considerations when it comes to cybersecurity in the medical space.

00:12:04

Michael: It's interesting as we're talking to all this, just recently, McKinsey and company put out another white paper, sort of around their basic premise, around the whole thing was that, hey, from 2012 to 2019, the med tech sector did a great job. They were outperforming the S&P 500. They were great return on investments for everybody. All that's great. But since 2019, all of that momentum has died down. And so one of their key recommendations that they have in there is that, hey, you should have like a digital version of your product, you should digitize your service in some way. And we're just talking through like the first of these issues.

But hey, that's not a just a thing. You just slap on that. That takes real thought, real requirement, as we're kind of thinking through, sort of like the difficulty and the cost and the consideration that needs to be given to this, given to these different matters. Usability is another one of the topics that we've identified here. What is it that is tough about usability? What are people not thinking of? I know that part of the answer is going to be they need to think about it early on. But what's the rest of the process there that people are missing?

00:13:09

Mohammed: The three topics that we're choosing are actually intrinsically linked cybersecurity, software architecture, and usability all trade off between each other and are all interlinked. So just to be clear,

they're not these completely independent things that you can just do one and ignore the others that turn it over to Andre for usability.

00:13:28

Andre: They're related in other ways as well, right? These are analytical processes that are being regulated or mandated upon companies. Right. Because they're good practices that they should be doing in the first place that lead to safer product and that companies that are very well resourced will do it. But precisely because there's so much interest in this space, so much investment, there's a lot of startups in this space coming in that really want to just hurry up and try to produce something and try to feel the product as urgently as possible. They may tend to cut corners in places where it's just not wise or safe.

So the regulations are there in order to try to guide us and prevent us from making mistakes that we're going to regret later on. Right. And that's true in cybersecurity and is just as true in usability. Whereas in cybersecurity, of course, you're trying to prevent somebody from coming in and harming you and attacking you, and they're stealing your data or harming a patient through a vulnerability in usability. We're, of course, always concerned with what kinds of user errors are possible from the various users of your device that will basically get them to harm themselves, right? Get them to do something with your medical device in such a way that really just that harms them.

And again, there's a set of practices dictated by human factors engineering that that are good practices that people should be doing in order to develop high quality products. And the FDA says, okay, well, I don't care how much of that you do, but do the part that is absolutely essential so that people don't harm themselves. But similar to cybersecurity, you ignore these practices at your own peril, right? You ignore these things at your own risk for usability. They ask you. You need to have a very clear intended use. You have to understand what this thing is intended to be used for. What are the indications for use for your device so we can understand who's going to use. This thing and for what purpose is and in what environments.

And you need to have that super clear because from that you need to be developing a device, designing a device that responds to that intended use and to those indications for use. And you'll be surprised. I mean, a lot of startups, other companies are so rushed into the solution space, they're so in a hurry to produce an actual product that they don't tend to sit down and think really about what this thing is going to be really used for. How are we going to delineate the space where it's going to be used for? Because there's a lot of adjacencies, and by you delineating what it's going to be used for, you're going to basically define the area of analysis, the area of design for your risks related to everything, really, not just usability, but usability practices are really just trying to drive you to that, to understand your users, understand how they're going to use the device in which use cases, and failing to do this analysis carefully early on in the process.

Again, I know everybody needs to do all these things as early as possible, but failing to do these things usually leads to disastrous consequences. On usually right, you end up having tremendous scope creep, lack of clarity on what the product is, lack of clarity, even the submissions. So by the time these things get to the FDA's hands, they look at this and they're like, wait a minute, you have 20 features here, but your indications for use in your intended use should require only three. What are these other 17 things

here for? And oh, by the way, you haven't done a proper analysis on the risks associated with those things. So why are they there in your device. So again failing to have clarity on these things and failing to follow this, these processes will get you in a heap of trouble.

00:16:49

Michael: Here's a conversation that that my boss and I have oftentimes, and I'm curious how it plays out sort of in your space. I come to him with, hey, here's a marketing plan that I have. It's targeting this person and this solution and this particular scenario. And he's sales guy by training. And so his response is, but why wouldn't we target all the people with all the responses and with all the different needs? So I'm sure that this is something that startups are trying their hardest not to fall into this trap. How do you guys handle that?

00:17:18

Andre: With a lot of patience. And again, by following the process, right? Surrendering possibilities is one of the hardest things in product development because everybody wants the best product possible, the widest scope possible that reaches as many different markets as possible. So surrendering that is, is one of the hardest parts of our job. And really the customers that are, I should say, the customers that reach success at the lowest cost tend to be those who are able to stay incredibly laser focused on what they're trying to do and are able to say no to the other things so that they can get at least one version of this thing fielded, and understand that from that one version fielded, it can expand into adjacencies afterwards. But trying to bite too much early on is usually a recipe for trouble down the road.

00:18:09

Michael: I'm sure it's hard to say no to anything more.

00:18:12

Jose: Part of it to part of our responsibility. And what we always try to do is just provide at least ballpark estimates of the impact on decisions to the overall project. So if they go, hey, we want to add this thing, it's not enough. So sort of qualitatively say, hey, that's scope creep. That's going to slow things down. That can have implications. If you become good at saying, okay, let's think through those implications. It's not because on the other hand, you've got to be careful. Sometimes there's good reason to increase the scope. And so you just kind of have to do that cost benefit analysis.

But if you don't present the cost in time and budget, then it's hard for people to make the correct decision. So being able to say, hey, here's how everything gets complicated by what you're asking for. It's going to cause us to have to go back and redo the architecture because of this and this. It's going to require us to do this kind of analysis. It's going to have to require this kind of incremental testing is going to do that. It's going to slow us down six months and cost an extra X number of dollars. Does that still

sound like a good plan? And then at that point they at least have data to make a decision, because as Andrés and Mohammed are alluding to, because everything is interconnected, right? The features, the indication, the cybersecurity, the usability, the indications, the like, everything is interrelated.

So once you've got a plan in place, if you start making adjustments, you've got to go back and evaluate the impact on everything. Yeah, it's that kind of analysis. And to Andrew's earlier point too, I mean, like you're saying, there's some products that people are very focused on the patient as they should be, but maybe they forget that the caregiver is probably a user of the system, or there's a doctor, there's a nurse, there's a technician, there's somebody at a reprocessing center. There's all these different players that may have to interact with the product in some capacity, and they might all have quite different needs that user analysis and task analysis that Andreas was talking about. It's a very practical exercise and it is depending on the product.

Some products are more than others, but for more complex products mean it can take weeks of very long meetings trying to think through idea, brainstorm, put together similar to what you guys do in marketing. Mike Michael around thinking of user personas, right? Like who are they? What's their educational background? What's their demographic background? What's what are important to them? What's their daily routine look like? All those things might be important in how you ultimately think about the usability of specific features.

00:20:35

Andre: In the space of the use of these devices, we tend to be concerned about dexterity challenges, mobility challenges, vision challenges, hearing challenges. Right. So trying to understand these personas, but in their full limitations so that we can make sure that we produce devices that are safe for them to use. And this is.

00:20:52

Mohammed: Particularly applicable when you look at. So when we talk about usability you have to consider also the demographics of the users mean. So it's one thing designing a medical device that's going to be used by young adults. And a different thing, if these devices are going to be used by the elderly, they pose different problems. And so and sometimes making one device that tries to meet both two disparate demographics is not the appropriate solution. So usability covers many aspects of this.

I'll offer one more with medical devices. There's the aspect of sterilization. If the devices require sterilization, how do you design them to be capable of being sterilized by potentially the end user as a patient, or if they're in a clinic by clinicians in their comments? I mean this again. So these are all uses, right? So when you think of usability and perhaps in a sort of more classical consumer sense, you're thinking of it really only with the intended user being the end user. When you think of usability in the which is which people can be familiar with, right. Because we're all consumers in the end, one way or another.

So we can have our own opinions about what a consumer thinks should have. But when you're that said, we're almost all non-medical people, so we're not physicians. So we're not don't necessarily have that

viewpoint. But when you're considering usability in the context of a medical device, as Josie said, you have many stakeholders and you have to be able to look at their viewpoints. And if you don't have that viewpoint, then you have to find people that do. And that's why you run trials and things like that so that you can actually get those other viewpoints. Because again, I think it's a mistake to assume that everything you'd be surprised to find how little when you ask people that actually do know. So it's just how it is.

00:22:41

Michael: Absolutely. I could dig into that topic a whole lot more. Let me jump to software architecture just so that we can kind of hit on all three of these just and this is something that we have been talking about quite a bit in terms of working with clients, in terms of what parts of it need to be sort of FDA recovered and what parts of it don't. Do you want to kind of jump in on that kind of quickly before we turn it over to our guests here, just in terms of how we're interacting with that space as well?

00:23:08

S4: We just had firsthand experience with one client where we built something that was all handling post procedural data, but there was a component around user login, which translated into there's an actual surgical robot. It performs cases in an operating room, and the doctor logging in needed to set up their account via this online gateway. So while it couldn't affect the procedure itself, it could limit their ability to start it by not being able to log in to the robot and finding ways of mitigating that. Because if we got into that classification, I think we're currently releasing every 2 to 3 weeks, like new software updates for this.

And they were saying that if this is part of your whole system, then you're going to have to switch to a much more stringent regulatory standard. And you could release software maybe twice a year. That would obviously be very detrimental to the business, to the physicians who are trying to use this system, engineers who are trying to handle this. If we couldn't roll out updates, that's a huge problem. And we had started down the pathway of maybe we would have to partition this one piece out and have it sit separately, be regulated separately, and finding those seams of partitioning your software seemed to be very critical to continuing business operations, while also adhering to the standards you need to.

We didn't have to in this case yet, but there is some exploration of pre procedural planning that we're exploring, and that one would almost certainly have to be housed somewhere completely differently in order to constrain that from hurting the business operations elsewhere. So that's kind of my familiarity with where you have to worry about these things. As someone who writes software that kind of supports or surrounds a device but doesn't write software for the device itself somewhat familiar with the topic in that regard, but I think you all probably have a bit of a different. And how does.

00:25:05

Michael: It fit with the context of a startup in particular? So we're talking about a device that's already on market. But how are startups thinking through this, not thinking through this? Enough. What were you guys seeing?

00:25:15

Mohammed: We're in the opposite side right. So we're from we're from the view. We're starting from the premise that the reason why we're engaged is because it is a medical. And that could be a physical device. It could be I'm developing I have a physical device, and I have potentially an application running on a commercial phone that's interacting with this physical device as part of it. You know, oftentimes this is a sort of a trend that's happened in the past, probably five, 5 to 10 last 5 to 10 years. And it's increasing, which is physical devices utilize phones as their UIs rather than putting a display on your device. I mean, in the old in the self-contained world, medical equipment would have its own little display and its own system and be completely self-contained. But these days, most people carry phones around, so why not?

It's very tempting to say, why not use the phone as a, as a display for the device? That's fine. But now your phone is now part of the medical device. And so we're starting from that nexus of okay, so I have a medical device. There's a physical component to it. There's potentially a phone that's now a part of this medical device. Somehow some application running on the phone is now a part of his medical device. And then it can go further than that. We can say, okay, well, the data from this is being sent up to a cloud. Perhaps it's being analyzed real time in the cloud. Perhaps there's a web view of that data that the patient also accesses from the other side. So all of that now starts to drag on and become part of the medical device.

And the medical device sort of tentacles continue to increase. So a start up thinking about all this doesn't understand necessarily where a medical device ends and where a non-word ends. The medical device data system starts. For instance, where does what do I what it falls within the regulation and what falls outside. Now? Now why is that important? Well, if you want to err on the conservative side and get approved by FDA, the answer is oftentimes simply we'll just include everything as part of the medical device. Because if we include everything as part of the medical device, and we go through all the rigor and we go through all of the processes necessary to make it a bonafide genuine medical device submission, FDA will be fine with it.

And you're probably right. They probably will be. But you've now taken a project that potentially could have been X in size and made it three x in size and three x in costs and three x and time. And so can you approach it that way? Sure. Our viewpoint is just not efficient. Why would you do that? We actually would tell our tell our clients, we can save you time and money if you want to approach it that way and spend a lot of money, you can. That's not what we would advise. You can save yourself a lot of heartache, a lot of time, and a lot of money if you are up front able. And this ties very much back into usability, actually.

And what Andre said about scope, if you are able to distill down what truly is the medical device functionality, what is the minimum functionality that the medical device actually has to have, and you're able to identify those boundaries that Justin said from the other side, right. So we're coming up and say

what absolutely must be medical device. And there actually are some rules around this that FDA, I mean, FDA has their own way of seeing if you're right or wrong, because they can test these boundaries themselves. I know what those rules are in terms of what they look for and what will pass and what won't pass.

And sometimes it's just as simple as, is there something you're going to be able to do across this boundary that's going to make this device completely change its behavior? If so, well, maybe that's not such a good boundary line. Maybe you've drawn the boundary to close. Or is it simply a boundary where you're just simply reporting some data that is non-medical in nature, in which case, yeah, you're breaking boundaries. Probably. Fine. Finding those boundaries, tightening them up, being able to make a clear delineation of what is medical and what is non-medical.

If you can do that early on, you can scope your project to be much smaller. You can get your submission to be much tighter. I think I personally, if I was a reviewer on the FDA side, I'd much rather review a submission with 500 pages than a submission with 5000 pages. So again, just human nature. So I think and honestly, the chances of you getting it right with a 500 page submission, I'm just using pages as a size reference, but the smaller the submission is, the better chance you're going to have of getting it right the first time. Unless it's almost like a security against, it's less of an attack surface for the FDA to look at and say, okay, hey, we found this one little thing in your submission here that we don't like.

Well, the smaller it is, the less chance they have of doing that. The bigger your submission is, the more chance they're going to have to be able to poke at it and tell you, go back and do this again and repeat this again, etcetera. There's definitely a business interest in making the medical device scope as small as possible. That is practical for the intended use of the device.

00:30:08

Jose: To touch on something that just to follow this with a concrete example like what you were just saying. Justin, part of the challenge that you face is not just the efficiency of developing the system, which 100% is a thing, but then it's also updating the system. Like you're saying, you want to do a release every 2 to 3 weeks. That becomes quite challenging if you have to do regression analysis and verification and validation and, and all those sorts of things on the new release. And if all you're touching are features that shouldn't be within the boundaries of the medical device, then you really shooting yourself in the foot unnecessarily if you inadvertently include them within the scope of what's the medical device.

Now that's where that experience and skill comes in of not only saying from an architecture standpoint, how do we divide the system components so that as much as possible sits outside of that boundary. But then like from a technical standpoint, two, as a concrete example, if you're developing an app that interfaces with a patient device that goes home with the patient, you may want to incorporate into that app a variety of features that are not part of the medical device. Right? I mean, you might want to send messages encouraging the patient. You might want to allow for the patient to have some sort of social interaction with others.

There's a variety of features that you can add to an app that are not directly linked with the essential functions, or the safety of the app of the of the device. And if you don't know from a technical

standpoint how to structure things so that you can divide those, then you're sort of forced into treating it all as part of the medical device, or you could be forced into that. So it's both kind of a regulatory understanding of that. Then it's also a technical understanding of how do you carve out components of a system to allow you to limit what's in the within the boundary of what's medical.

00:31:46

Mohammed: And if you tie that, you can just bridging over to what Andre said about usability. Right. So you consciously are thinking about literally separation of boundary separations, right? You run the risk of getting poor usability because you end up with distinct systems. So you've got distinct parts of this thing. But from a potentially an end user perspective, they're not interested in the fact that you have a boundary. They're looking at this as a whole thing. So again, you have to balance all of that. So to Jose's point okay, we could solve the medical device app problem by just having two apps. I could have one app that is for my medical device and that's the medical device app. It's tiny, it's small, just it has two buttons in it and one display.

And that's all it does is very limited. And then tell the user this, you launch this other app to do your surveys and all the other things. That's a solution. Is it ideal from a usability perspective? No, I'd say the user probably doesn't want to have to remember. They have to launch two different apps to do two different things. So then how do you do that? How do you create a single app and a single app experience to the user, but internally divide it so that the FDA sees the medical outside of the medical clearly as a delineated boundary. And that's one of the things that we've learned how to do over the years. Really good systems.

00:33:04

Michael: That's awesome. Guys, it seems like each of these things that are interconnected. Thank you for clarifying on that, but how interconnected they are made. It'd be great if you just had infinite time to just keep on playing with each of these things, but the whole context in which we're talking about here is startups speed to market, speed to getting distribution speed to getting out there. And it's so critical for them to be able to continue innovating. So guys thank you so much. Obviously they can find you guys at Bold Type and ask you all the many more questions that I'm not asking right now. Is there any one thing I guess you would leave with startups, as they're kind of considering how to approach all this? What would be like the one piece of advice that you would give them if you.

00:33:45

Jose: Focus as time to market, don't cut corners early, especially like the really good high level stuff like your user analysis, your task analysis, your cybersecurity analysis, your usability stuff. It's important to do that stuff early, and it's a process that will really help you understand what the requirements need to be, which is also one of those things that is just necessary to do as part of design controls. So don't think that you're saving time. You're actually probably going to cost yourself a lot of time if you don't do those things early. So just you can be efficient and still follow the process.

00:34:19

Mohammed: It's sort of counterintuitive, but it's the old adage of sometimes stopping makes you go faster. Yeah, it's one of those things, right? It's stopping up at the beginning of your project for a month to figure out all of these details and come up with a really good approach, and a really good plan will save you dividends down the road, because without doing that, you're just going to dive into it and then discover six months down the road that you wish you'd spent the time upfront figuring this stuff out.

00:34:44

Michael: Absolutely.

00:34:44

S4: I would imagine an FDA rejection and scrambling to address this a massive that's.

00:34:49

Mohammed: Even worse then you've lost. I mean, when you think about the time that now that's even worse because think about the rush. You spend six months a year, whatever it is, and now you get to your submission and now you have to wait. And you sit there waiting. And if they don't approve it first time, you've just wasted all the time waiting and you've got to reset. And then wait.

00:35:08

S4: Again. Who knows what Remediations is?

00:35:12

Mohammed: Exactly. And your goal really should be spend the time upfront. Think it through. Do it once. Submit it and get approved the first time. That should be your goal.

00:35:21

Andre: I'll just add one more thing and use pre subs to make sure that what you end up submitting addresses the concerns that the agency will have. So if you can do your pre sub to understand what their concerns are, make sure that you do the work to address those concerns. Your life will be a lot easier at the other end, but if you're rushing rushing you don't pre sub you submit. You just basically yeah you're in for a surprises.

00:35:44

Jose: It's a great point. And coincidentally we just launched two blogs in the last month and one of them is on pre submissions. And why you shouldn't avoid them. And the other one is on cyber security. And why like FDA will refuse your product or you refuse your submission due to cybersecurity issues. So on the website you can find those awesome guys.

00:36:02

Michael: Thank you so very much and everybody that tuned in. Thank you so much for your time today.