Webinar Transcript: Essential Cybersecurity to Protect Sensitive Clinic Data Webinar

Jillian All right, thank you so much for joining for this Essential Cybersecurity to Protect Sensitive Clinic Data Webinar. My name is Jillian Maccini with the RHNTC and I am delighted to have you here today. Just a couple notes before we get started. Everyone here today is muted, given the typical number of participants that we have at events. We do plan to have some time after the presentation for your questions and we will take questions throughout, so please don't hesitate to participate in the chat. At any point we can talk about anything that you like. So do put your questions in the chat whenever they come to you, no need to hold till the end. Closed captioning has been enabled for the meeting and to view that you'll just click on the CC icon at the bottom of your Zoom screen. Nancy's going to chat out the evaluation link. Your feedback is super important to us and has enabled RHNTC to make quality improvements in our work based on your comments. So please take a moment to open the evaluation link in the chat and you can complete it in real time. You can just have it open so that it's ready to roll whenever you leave the session. Including right at the end. So please do take a moment and open the evaluation now so that you can complete it whenever you leave the session and so you don't potentially miss it and we sincerely appreciate your feedback. This presentation is supported by the Office of Population Affairs, OPA. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of OPA. And with that, I will see if I can successfully share my screen again. And it's not gonna be correct the first time, but we're gonna get it correct here in just one second. So let me just fix it. And there we go, great. Okay, so let's go ahead and get started. I am joined by my colleagues, Sarah Cruthirds and Lisa Schamus, who may join in as well in the conversation, but they'll be in the chat with you sharing their experiences when that's appropriate. So thanks for being here, Lisa and Sarah.

Jillian All right, so as I said, I'm Jillian Maccini. I have been the FPAR 2.0 lead for RHNTC for a couple years now. I was gonna be joined by some other folks, but the best laid plans oft go awry. And so it is just me here today, but I'm really looking forward to chatting with you all about this topic.

Jillian So what brings us here today to quote Princess Bride is family planning clinics really need to be very, very cognizant of cybersecurity threats. I think often small clinics, small programs, small programs within larger institutions, within larger health systems or health departments may feel like they're not big enough to be a target of cyber threats or maybe feel like the sort of onus to manage those threats sits elsewhere. And I really want to stress that I don't think that's the case. Clinics and administrators really can take proactive steps to protect your clinic, your clients, and data, and to continue to provide services. So I'm going to pause and ask you all to share in the chat what you think, like what is your, what do you think makes it

tough to consider or reckon with the cybersecurity threats that might exist in a smaller clinic, in a family planning program, in a department within a larger clinic. What do you think can make it hard to reckon with cybersecurity threats or risks in a small clinic or program? And you can put your answer in the chat and that will just help inform our conversation as we go forward. And Sarah has summarized that in the chat. Thank you. And we're gonna give folks just a minute to put some responses in. Yeah, Audrey says turnover capacity. Yeah, Camden makes a great point that the tech literacy of staff can be really variable and that that is fairly important when we think about these things. And especially if the decision makers have somewhat less tech literacy than maybe we would ideally want. Raymond says limited tech budget. Yep, absolutely. Sort of, and that can be like perceived, real, and tech budget can be money. It can be time to spend on it. Resources aren't always just money. So that's a great point as well. Yeah, so I think you all have really touched on these key things that I think can really make this feel like something that doesn't necessarily end up in the middle of everyone's primary consideration.

Jillian So let's jump in to what we're gonna talk about today. We're gonna start with a case example, and then we are going to talk about minimum roles and responsibilities, then we'll move on to talking about important considerations for remote staff. And when I say remote staff, I don't necessarily mean staff who are working from home. It can just be staff that are remote from central services, right? From your central IT staff, from central support, who might be able to help with some of those things. And then the role of IT support, sort of who might we turn to, what might we need to know from those folks in order to prioritize some cybersecurity activities within our own clinics or within our program.

Jillian So our objectives today are to apply some basic security practices to safeguard our systems and connected devices, really thinking about whatever computers, laptops, desktops, whatever you use to access your systems and your EHR itself, as well as any ancillary devices or services that are attached to those things. We want to identify some common risks when managing confidential data and some simple, and simple in quotes, Ways to avoid those. And then grasp some core ideas behind preventing data breaches and what to do if one occurs. A data breach is my worst nightmare in this space. And I suspect it is for many here as well. And so really that's sort of what's center of mind in this conversation is how do we prevent that from happening and sort of, what do we do if it does? And then implement some simple settings to protect networks from unauthorized access. Sort of take some initial steps that we can take with limited budget, limited capacity, all of those things to protect our data to the extent possible.

Jillian So there's a really important and somewhat tricky balance when we talk about the importance of securing sensitive patient data and preventing data breaches, right? We have regulations that require this. This is HIPAA and all that it encompasses. It's requirements around having sort of your incidence response plans, that sort of thing. There's also regulations around what Title X encompasses and requires, as well as state regulations. And so that can have lots of implications as to what we're required to do, sort of what paperwork we're require to do. As well as sort of how we have to respond to things. Then we have reporting requirements, and this can be grant reporting, this can all sorts of things, which require us to collect certain data that is sensitive, right? This comes up very often that, you know, as a family planning clinic, we might be collecting and recording information that could be considered sensitive by patients, by

others, and sometimes the reporting requirements such as FPAR. Include some of those details. And so therefore we are having to balance sort of, okay, we are collecting these data, but it does make it more risky or we feel like there's a bigger risk around those data breaches. Then we have sort of privacy and security, right? This is important for reputational reasons. This is for patient safety reasons. This is is important for continued operations and trust. Privacy and security is really at the heart. Of everything that we do, and then we have efficiency, right? Continuing to provide care, even in light of these competing demands and concerns is a real challenge. So when we think about sort of what it takes to balance all of these things, I think we can often, you know, sometimes we're deprioritizing one in order to prioritize the other. I think many of us have maybe worked with a compliance person who was a real stickler. And so maybe efficiency was slightly lesser. And then maybe sometimes we've worked with someone who's all about the efficiency. And so sometimes the regulations aren't at the forefront. And that balance is really important to acknowledge and understand as we're talking through these things.

Jillian So let's jump into our case example, which is Healing Hands, a fictional Title X clinic, and they've had a cybersecurity incident.

Jillian So a little background on them. Uh, they are a Title X clinic that's part of a larger primary care clinic. The project is staffed by a provider, two nurses, and a CHW. The Title X staff access the shared EHR, and when I say shared EHR, I mean shared with the larger primary care clinic via dedicated laptops. And their larger primary care clinic has many sites. The Title X project is not located at the main site. So it's like further afield. Not close to central services, as I was mentioning earlier.

Jillian So, the cybersecurity incident here is Sarah, a new nurse at the Title X clinic who primarily provides STI testing, who just started very recently, received a phishing email disguised as an urgent security update from the clinic's EHR. The message included a verified credentials link that led to a convincing fake login page. The breach happened when Sarah entered her username and password, which were immediately harvested. And the outcome is that attackers gained access to the EHR and cloud storage. And the attacker objective in this particular situation was data exfiltration, actually downloading that sensitive patient and financial data, not ransomware. Certainly we hear lots and lots of ransomware examples from phishing attacks of this type. But in many cases, we are also seeing this type of data exfiltration where that data is downloaded and then released online for nefarious purposes or sold to bad actors, that sort of thing, which is a horror show. Like, let me just say that. I say that like it happens every day and it does, but it's a horror show.

Jillian So the fallout in this particular clinic was that the breach was discovered two days later by Dr. Anya Sharma, the medical director for the whole clinic system. When Dr. Sharma noticed unusual activity in the EHR system logs, specifically large data exports originating from Sarah's account shortly after Sarah got access to the EHR because she had just started. So, you know, maybe there's a clinical informaticist somewhere in this clinic that might do that type of

downloading of the data, but Sarah's not that person. And a subsequent investigation confirmed unauthorized access and data exfiltration. So there had to be a temporary shutdown of digital systems, including EHR and email, and then reliance on paper records for days, which slowed intake, medication, referrals, et cetera.

Jillian Sorry. So what were the root causes of this? When we think about why this happened, what exactly happened there? Let me just get to where I'm going, I apologize. So first thing, lack of formal training seems like it could have been part of what happened here. While basic computer use was assumed. There wasn't structured or mandatory cybersecurity awareness training for all staff members, especially regarding identifying phishing attempts. You know, I think, especially if we're sort of facing a lot of turnover, as someone mentioned in the chat earlier, that onboarding process can become more abbreviated or can become, again, deprioritized. And so that lack of formal training can happen. Also, weak password practices and the absence of multi-factor authentication, right? So Sarah got this, and I'm talking about Sarah in this case example, well, my colleague Sarah's here, it's not this Sarah, I promise. But, so this phishing attack had a link and it said, you know, you have to go here to verify your credentials, and then they were able to access the EHR and the system just with those credentials, which means there was not multi-factor authentication, right? So, multi-factor authentication is not perfect. I'm sure folks in the chat can tell some stories about things that they've read and that sort of thing, but it is a really, really good step to eliminate the ability of folks to get into your systems. And so, multi factor authentication can be through an SMS text, like we're all very familiar with, can be though authenticator apps, or through email. There's lots of different options here, but Sarah had a reasonably complex password in this case. But the clinic did not require multi-factor authentication on its cloud services. Had that multi-factored authentication been enabled, even with compromised credentials, attackers would have been faced with like that additional barrier of not having access to that device or service for that multi factor authentication and it likely would have stopped that. Also, insufficient access controls. Sarah's administrative account had broad access or permissions to both the EHR and shared cloud storage, which really sounds like it exceeds what was strictly necessary for her role. And this is very common in small organizations, right? We have so few people that we need to make sure everybody can access the things that they need to access, but that sort of privilege creep really does allow attackers to exfiltrate everything with a new nurse's credentials in this particular situation. And so there just aren't enough access controls there. And then a lack of incident response plan. The clinic didn't have that incident response plan or this team that experienced this didn't know about the incident response plans. Which led to confusion, delayed reaction, and a reactive approach rather than a systematic one, which does exacerbate the impact. This could be particularly likely in a smaller program within a larger clinic, such as a Title X project or program, because folks might not be at the table for those discussions of the incident response plan. That might be something that's done in the IT department or done elsewhere in operations, and, you know, the- the Title X staff may just simply not be aware of it when it's really critical to be aware it. And then limited IT resources and support. As someone said in the chat earlier, as a small clinic, Healing Hands relied on an external part-time IT consultant for technical support, but not for proactive security policy development and continuous monitoring. And then the last sort of root cause that we can identify here could be a culture of deferring to experts. I think this is something that comes up a lot where we're like, I'm not an IT person, I don't know what to do. Or, you know, I did this thing, but I don't know, you know I'll need someone else to tell me what to do as opposed to sort of proactively saying, I clicked on this and once I entered my information something strange happened and I need, you know, need to

make sure that that's resolved. And I think we can all be familiar with all of these causes. So, you know, they're sort of portrayed as something that's quite negative, but these are all very common and reasonable. So what of these resonate with you? What of these do you think about when you think the importance of preventing a data breach, securing your patient data? What of the six potential root causes? Resonate with you and feel like oh yeah that's a that's the thing that we constantly have to make sure we are working on. And I should have made this a poll. Analise says all of them. I mean yes definitely I agree. What do others think? And if there's one that you're like, I actually think we're doing a nice job on that, we recently made sure that everyone's using multi-factor authentication, we recently added cybersecurity training to our onboarding, that sort of thing, please throw that in the chat as well. Christina says limited IT support, yeah, absolutely. Culture of deferring to experts, definitely. No one wants to take ownership, even though as the IT person, I have no problem fixing it for them if needed. Camden, I want you to wear a shirt that says, I'm here to help. We will whip one up for you and send that over. But yeah, I think it's a really interesting point where I think you're saying from your perspective, that's what you're there for. And from other people's perspective, it can feel like I'm going to get in trouble if I do this or if I say that this happened. Annalise says they are working on strong passwords and two-factor authentication across the agency but still have work to do. We all have work to do, all good. I love to hear that this is happening, though. And the other thing that I want to say about what Annaliese is saying here in the chat is strong passwords in two-factor authentication are a nightmare. Like, they are the things that make your providers mad at you. They're the things that make your staff want to throw their phones, like, I get it, I feel the same way, we probably all feel the same way. But this security does really matter. So, you know, do we bring everybody to a rage room and let them get it out while we talk about how we're going to implement this? Maybe, but we do really want to highlight why it matters, even though it is a total bummer to implement. So that's great. Thanks for sharing that. Once again, I've lost my cursor.

Jillian So then the other thing I wanna ask of you all is what is the role of staff in addressing these issues that we just talked about, these issues right here? What is the roll of staff in addressing them? How can sort of we all assist in addressing this? And Sarah, I would be interested in hearing your perspective here as well.

Sarah Yeah, I'd be happy to provide that. So just as a little bit of context for everyone, before I joined JSI, I worked at, or RHNTC, I worked a health center. So could be similar to some of your settings in that it was smaller and that a lot of people wore a lot hats. So I think for us, like when I think about I think that organization was very behind in its approach to cybersecurity simply from a competing priority standpoint of we were not actively within a data breach, we were actively suffering a cyber attack and there were five million other things to be looking into and working on and doing. So, but I think something that resonated with me from the previous slide was Um, and just from the example that you had was somebody having lots of access to like lots of different things because, Oh, they, they might need it or we need, you know, backup in whatever, whatever the case may be. Um, you know, that, I think that they got it.

Jillian They got it when someone went on maternity leave and it would never roll back.

Sarah Never rolled back. Yeah. And so that was definitely something that I now that I think about my previous organization that I think could have been done better. I know from day one, when I started working there, I had access to almost everything. Yeah, I was, you know, young and just out of grad school at the time. So thankfully, nothing happened. But that can't be the prayer cannot be the attitude that we take with cybersecurity awareness.

Jillian Yeah, yeah. And you make a really good point that there's also, and I think folks in the chat have mentioned this as well, but there's this circumstance in which there are so many fires to put out, or however we want to frame that, in many, many clinics that if it's not actively happening, it just is tough to prioritize. And I think that's very fair, but it also is kind of a recipe for trouble in some cases. Really, I hope that this case highlights the intersecting roles and responsibilities that everyone has. Really want to highlight that cybersecurity and really preventing these data breaches is not solely an IT responsibility. It really is a collective effort. All staff members, regardless of their role, really do play a critical part in maintaining our ability to keep doing what we're doing, our ability keep our patients. And their data safe, our ability to keep ourselves safe and functioning, right? And that we really do have to think about those root causes each in our own roles beyond just sort of we let IT take care of it. So hopefully that illustration is helpful.

Jillian So let's think a little bit more about those roles and responsibilities as we seek to minimize future cybersecurity events or I'll say data breaches or cyber threats.

Jillian The number one thing I want everyone to take from this part of this is that cybersecurity is patient safety, right? Our ability to take care of our patients, to care for our clients in a way that acknowledges their past through their historical record, all of that sort of thing, to prevent adverse events of all sorts, anything like that, cybersecurity really is patient's safety. And I know sometimes we talk about going back to paper records as if that's a dream, but from a patient safety perspective, that is not what the evidence says. So really important to think about that.

Jillian So some minimum roles that we really need to think of. And these are not roles that are gonna be within your Title X program or project or clinic, but typically they're gonna be in the larger clinic, right? And so this is going to include management, who's going to develop policies, manage all support and training, and provide strategic oversight. We're going to have some EHR support. This might be within the larger organization. This may be from a vendor, this might be contracted. But that EHR Support will typically lead optimization, user support for the EHR and other digital health tools, that type of thing. We'll have IT support, who will handle IT troubleshooting. Hardware and software support, network maintenance, that sort of thing, we'll have cybersecurity and compliance, and that person or that role will handle security assessments, key cybersecurity tasks, ensuring regulatory compliance. And there's a really tricky balance here, going back to something that I said at the very beginning between handling regulatory compliance and really being ready for when something happens, like we just

described in this case example. And then we may also have some outsourced services. So this might be managing IT functions that are sort of like discreet, maybe as we're rolling out something new or could just be sort of other things that are outside of the in-house capacity. And then everyone else has a key role to enact the guidance provided by IT and cybersecurity. So. Again, these are not going to be a bunch of new FTEs that you have, but rather you do need to know where these responsibilities live in order to know where to turn and what support or hierarchy exists. Right. So if we think. Our EHR doesn't have multi-factor authentication. Sometimes we just think that that's the case because someone said something one time or that sort of thing. We really do need to know who we go to for EHR support to ask that question more specifically as of today's date, right? Things change, technology changes, all of those sorts of things. If we're having trouble getting into something, rather than Googling around, we need to know who to go to within our own clinic to get answers that are specific to our clinic. And so that's really what I'm saying here. Again, not that you need to have a bunch of new FTEs, but that it's really important for everybody to understand who holds these roles so that you know where to turn.

Jillian So then again, thinking about this small, these sort of small clinic challenges. Sometimes we hear, you know, I'm kind of in this alone. I am out here. I'm doing the best I can. So a common question that we hear especially from these smaller clinics or those with limited IT staff is, what if I am handling this alone? The good news is you're not entirely on your own. Computers do some of it for you. And there is sort of some agreed upon processes here. And so the first action the single sort of most effective and cost effective thing you can do is patching, which just means applying updates in a timely manner. And so we may all experience patching as that like alert that shows up on your computer telling you you have to restart overnight, which again, total nightmare, right? But this really is the most important thing. This really is thing that sort of prevents uh... Many many breaches. So this is not a one-time project. It's an ongoing task that might take a few hours a month. It's about building that regular habit. Think of it like regular clinic maintenance, checking on things to make sure they're running smoothly. From a cost perspective, the financial cost is typically pretty minimal, if anything, because these typically are sort of pushed out by the programs that you already have, whether it's... Microsoft, if you've got a Windows machine, whether it's your EHR, those sorts of things. The biggest investment is typically going to be the time that staff spends on it. So what is the sort of why behind it? When a new vulnerability is discovered in software, again, like Microsoft or even your antivirus company, even your EHR provider, they release a patch to fix it, right? They release a little update, this is why we have version 9.1.0.4, and then 9.1.0.5 is because these are these little updates to fix these vulnerabilities or issues within the software. Cyber criminals, people who wanna steal things, actively look for these known vulnerabilities because they know a lot of people won't have applied the fix yet. If we put off patching, that means we have this open door, and once the vulnerability is known, we have to assume good and bad actors know that that vulnerability exists. And by regularly installing those patches, those updates on your operating systems and software, you are essentially sort of closing that door to those attackers, and it's really a proactive way to prevent security incidents before it can even start. So I have a question for anyone who wants to share their thoughts. And it is, when we talk about these things that we know take time and... Mostly time, but also just like being out of the system that frustrate staff, what are some ways that we can encourage people to do those things to smooth the process for that? And again, thinking about multi-factor authentication that we talked about before, thinking about stronger passwords that we've talked about, and thinking about making sure that patching is done in a timely manner. How can we engage people to

make that like just easier to do? And folks, I think Nancy can tell me if I'm wrong, are welcome to come off mute and share their perspective. But yeah, when we think about this as a staff question, how do we engage staff to make sure that they're doing these things? What are things that can be helpful for that? Katie says, rewards and avoid penalizing for time lost to do these things. Yeah, that's a really good point. Like if you need to get a visit in every 15 minutes and then it takes 15 minutes to get into the system in the morning, yeah. So avoiding penalizing and providing some rewards. Analise is saying, share risks and potential consequences, make it matter. Absolutely. Camden says, I have created auto patch updates for most of those things through Intune. Great. And Nancy's telling me you can't come off mute, so I apologize for saying that. And Raymond says, you can automate a lot of these functions to occur after work hours. This is true, but I think if people shut off their, so if you're me, you always take your laptop downstairs at the end of the day, and then you shut it off when you're done working, and then all of a sudden it's six days later and you have not installed the patch. So. You know, just putting myself out there as an example of bad behavior. So, oh, Camden says we have our patches set for during lunch hours. So that's helpful in the example that I gave, but also, you know, potential source of frustration if folks, you now, are supposed to catch up on their charting at their lunch hour, that sort of thing. Lisa, what do you have to say?

Lisa I think that most people who are here are here because they really, really care about their patients are very mission driven. I think just driving home that point that it's really about the clients and protecting the clients. And yes, there's a pain. And it's being kind to our clients. Yeah.

Jillian Yeah, I think that's a really good point. And from the strong password perspective, which is something the last time we talked about this with a big group that came up a lot, because people really have a hard time remembering their passwords, managing their passwords coming up with new passwords, that sort of thing, which I certainly understand. Pointing out that there are ways to resolve that, you can use a password manager. You can you you know, there are protocols that you can use. You can use a pass phrase that updates, you know. Winter is coming, 2025 exclamation point, combines both your John Snow and your need for a pass phrase. You know, so something like that, like sharing those sorts of like tips and tricks that can be used, I think is also really helpful because even when people are super well-intentioned, they can be overwhelmed, right? Raymond says, communications is key. Tell staff what you're doing and the importance of doing it in a timely manner. Yeah. And then. I do think as folks said up above, making sure that we're not penalizing, we're not getting people in trouble for being slow and instead using coaching, motivation, that sort of thing to move folks forward on these things is super important. Yeah, Sarah says creating a quick cheat sheet with those facts and methods really makes this easier. A little cybersecurity cheat sheet that is like part of onboarding to be like, here are the things that you need to look for, here are things that we're gonna be expecting you to do and we really need to make sure we're doing those things and here's some ways to make it easier. You know, if the patches come out Wednesdays at 12:15, making sure people know that and making sure that schedules allow for that. Those two things both need to happen, is a really big part of this. So yeah, that's great. And I do totally agree that communications are key, incentives are key all of that.

Jillian So the second action is installing antivirus and firewall protection. I'm almost certain everyone has this already, but keeping it updated, making sure that folks are only accessing your systems through devices that have that, very important. Personal devices become really risky when we think about this. So again, probably done by central IT services. Sounds like we have some folks who do some of that here. And so your role might only be to keep it up to date and to make sure again, that you're only using those devices that have that updated antivirus and firewalls. Again, not using personal devices to access clinic systems, things like that is really important. Time commitment, this is not an all day or all week task. It'll take a few hours to initially set this up on all of your computers and devices. Once it's in place, the tools really do do a lot of the work for you. And the cost is not super high. Many effective solutions are sort of like $50 or less. And there are some reputable free tools, though I remain skeptical of many free tools. And this investment really can save a lot of time, money, and stress down the line if a breach were to occur. And depending on the nature of your organization, you may have like cybersecurity insurance or cyber liability insurance, and that will have certain requirements of what you need to have. And so that's an important thing to have a conversation with your central services about if your sort of organization is big enough to have something like that. And so why is this important? Anti-virus, anti-malware is really sort of a security guard for each individual computer. It's sort of constantly scanning your computer for malicious software, things like viruses, spyware, ransomware, and detects those threats and prevents them from running on your computer. In our AI age, these things are evolving really, really quickly. And so I think. Again, this is another reason these things are really, really important as a first line defense. And then a firewall is like a security checkpoint for your entire network. It's a barrier that controls what information is allowed to sort of come in or out of your system, right? It can be a dedicated service or a feature built into your network router or operating system. And its job is really to block that unauthorized access and suspicious network traffic. And the reason these two things are important together, is because the anti-virus, anti-malware is for your individual computer. And then the firewall has that sort of same defense but for the network as a whole. So you have these like two walls that anything has to go through that becomes really important.

Jillian And then, the third action is, so heaven forbid everything we've talked about so far fails, which it does somewhere every day. You need to have backups. This is your last line of defense. This is really, if everything else fails, a good backup can be the difference between a, you know, bad situation and a complete disaster. And your time commitment, the initial setup for a good back up system might be about a day, you know, considering we all get interrupted endlessly, maybe it's a couple days. But it involves setting up the software, choosing a backup location, and running that first full backup, which can take a long time. But after that, it's about checking and testing those backups periodically to make sure they're working. You really do want to be confident that when you need to restore the data, it is there and readable. I recently, I guess it was probably six months ago now, was at a conference where there were two cybersecurity presentations. One was a clinic that was like, here's what we did, and it went really well. And one was a clinic that was like, here's what we did. And it was a bad situation. One had downtime of like a day and a half, and one had down time of like, a month. And when we think of that from a financial perspective, from an operational perspective, from a reputational perspective, it's catastrophic to be down for a month, right? And sometimes we can open back up on paper, you know, those stories certainly exist. But our best case scenario is to have that good backup that we can restore to. It's there, it's readable, we can access it. The cost here is not low, right? The server space, the hard drive space can be expensive depending on what we're thinking about. And a cloud backup subscription, which is often what we are gonna

do, is ongoing. So it's a monthly expense to add to what is often many other monthly expenses. But it is really critical. It really is the difference between sort of being able to continue and not being able to. So why is this important? A backup is that extra copy of your important files and patient records. So an offsite or cloud location is generally recommended because it protects from physical threats like fire, hurricanes. Anything like that, as well as being useful in instances of cyber attacks or ransomware. And ransomware encrypts your files, making them unreadable until you pay a ransom. And if you have a recent encrypted backup, you can simply wipe your machine or your system and restore your data without paying the attackers. There's a lot more to unpack there, but that is the thought anyways. And then encryption really is key, even if your backup drive is lost or stolen, the data on it is unreadable and until someone has that encryption key. And so that's really a critical step as well. So the system that you're working on is encrypted as is your backup. That's really important. So those are sort of the walls or the barriers that we can put up to bad actors getting access to our data. So, preventing those data breaches.

Jillian Um, with those steps completed, you are in a fairly good position to withstand lots of cyber attacks. But unfortunately, as we discussed in our case example earlier, the staff or employees really can remain a point of weakness, even if we've done all of the other steps. This is because staff can be targeted by phishing attempts. Again, phishing is when an email or text looks like it's from a legitimate source. But actually seeks to steal login or credentials or otherwise gain access to systems. Phishing is very, very, very common and seems to be getting much more sophisticated and targeted with the use of AI. So for that reason, staff really need to be extra vigilant. So how are folks in the chat training or communicating or testing or quizzing or whatever around phishing? So what are you doing to increase staff awareness about phishing? And there's some answers on the screen so you know you could choose to use those, but I want to hear your experiences. And I so appreciate hearing from all of you in the chat. It's always really, really helpful to have these sort of grounded examples that you're sharing.

Jillian And we'll give folks just a minute.

Jillian Yeah, Analise says, we get a lot of random phishing emails and share examples with everyone in the all staff chat to keep those spidey senses activated. Paige says we get quarterly quizzes from our IT department that are mandatory. Are they like quiz quizzes or is it like blind tests and you have to not click on it? Raymond says we subscribe to InfoSec and they do quarterly trainings online. Camden says, we made an addition to the company handbook that includes all types of viruses and what to look for and how to avoid things. Yeah, those are great. Other companies are like KnowBe4, they have training. Paige says, some are blind tests, some are short visits, videos, sorry, that have quizzes afterwards. Erica says, our department has awareness drills. I know, I certainly, we get tests, phishing tests, and if you click on them, you have a mandatory training you have to do within five days after you click on them. I only did it once, let the record show, but it is really helpful. And so it sounds like some similar things that folks are doing here. Yeah, that's really helpful, so making cybersecurity a routine part of staff education, I've said this several times now. But making sure that that's part of your onboarding security training for new hires, requiring all staff to attend at least annual training, very similar to what several of you have shared in the chat, and making sure that we're using non-technical language and real healthcare examples for this so that everyone can sort of understand their

role. Again, I think it can be very easy to feel like, this isn't me, this isn't my role, I don't have anything to do with this. So again, making sure that we're using that non-technical language and really specific examples. Phishing awareness and drills, training staff on how to spot red flags in emails, including looking for suspicious sender addresses, spelling errors and unexpected attachments or links, urgent or threatening language. Urgent language really being a big one to look out for. In healthcare, I think most of our urgent communication does not happen via email. So when there are urgent emails, that should sort of immediately throw up people's spidey senses, as someone said in the chat. And then periodically running phishing simulation exercises, sending out fake phishing emails or real phishing emails that are fake emails to see who clicks and then use the results as reinforcement. Again, going back to what someone said earlier, about rewarding those who do the right thing and not penalizing those who don't, but rather using it as an opportunity for training. So congratulating those who report the phishing email and providing a quick refresher training to those who were tricked. I have had to do the quick refreshener training. It really is useful. Sarah, you just haven't been here long enough.

Jillian So some keys for staff engagement. We talked about this a little bit earlier, but things I really wanna recommend are encouraging a blame-free atmosphere where employees immediately report potential security incidents or mistakes like clicking a bad link without fear. I thought Camden shared something really helpful earlier, like this is what I'm here for, come to me. And really encouraging that blame- free atmosphere I think is really important. Providing easy channels for staff to ask questions. Give people a way to take a screenshot or a cut and paste and say, is this legit? And that someone will respond to them because otherwise they'll be like, oh my God, well, I need to open it because what if it is? That becomes really important. Using engaging methods to keep awareness high, whether we're sharing monthly tips, news of breaches or questions to spark discussions, what someone mentioned in the chat about just like sharing examples as they come up to make sure that folks know that this is sort of an ongoing issue. And then again, remembering that the goal is to highlight cybersecurity into daily work routines, just like hand hygiene, right? Cyber hygiene, hand hygiene cyber safety, cybersecurity is patient safety. Those are very similar in that way.

Jillian So just a couple last things for us to chat about. One is a checklist for anyone who is working away from the main site.

Jillian So more than just working from home, working remotely can mean providing services at a school and using their wifi or being in another location where you're using wifi that is not the clinic's wifi or using, you know, checking messages at home after work hours, that sort of thing. The checklist that Nancy just chatted out, I'll see if I can open it. Hopefully nothing blows up. Let's see, change my sharing. So this is just a checklist that can actually be printed out. Let me present it. No, I'm doing the wrong thing. That's okay. We're going to go like this. So this truly just a checklists that can be printed out and shared, it's about securing your wireless router. Really important for people who again are working from home or somewhere else where there might be shared information. Securing your computer and devices, and this is really intended to have like sort of plain language can be handed out to anybody who's working remotely and then making good choices when working remotely, and educating others. And again, we can be talking about working from home. We can be taking about working from a school from another

location where co-located services might be being offered, anything like that. Let me switch my screen back. Oh, I knew I wasn't gonna do that correctly. I apologize. And one more time, so I'm back at the beginning. Hang on. Here we go. All right. Let me just scroll forward, I apologize.

Jillian And then the other thing to consider is that, thank you, Christina, is that we're not always gonna be able to do it alone. Like when we think of all of the responsibilities that exist to do these things that we've said, good, mission-driven, lovely, wise people can do a lot of this, but can't do all of it, right? So there may be situations where you need additional support and that is like perfectly reasonable and fine. It's really important to make sure that you are turning to trusted colleagues or associations in your field or area. I'm thinking if you are part of a health center, your primary care association may have some recommendations, maybe something like NFPRHA or something like that. Lisa, have you heard of any discussions around outsourced IT services for family planning programs? It's okay if you haven't, I'm just asking. Okay, but you do wanna make sure that you have like sort of an interview approach or the RFI or RFP that you put out if you are really looking to contract with a consultant. Make sure that it has some of your family planning or Title X specific considerations in it so that you can be sure whoever it is that you may hire has the knowledge of things that might be particular to your clinic, to your program, that becomes really important. I also am really interested in like shared models. You know, I know many instances of shared CFOs, shared CIOs, that sort of thing. I think there may, I think, there's interesting opportunities to do similar things, but that's for everybody to decide whether, how to sort of set that up. And I understand that from a contracting perspective that can be really challenging. But if we have really limited staff, some might consider a virtual or fractional CIO or CISO to assist with gaps, or to get an IT consultant to set up a new training program, or maybe you're contracting, you know, someone mentioned InfoSec, I mentioned KnowBe4, those can be sort of contracted services that you can use for some of this as well. And again, this depends on your structure. Like so many other things, you know, depends on what resources you have available for these purposes. Uh, the other one, Analise is KnowBe4.

Jillian And I will get the link while folks share what is one thing from this discussion that you can implement in your clinic or that you would think about implementing in your clinic or that your thinking, oh we actually might need to do something a little bit different there.

Jillian Here is. All right.

Jillian Sorry, I went to copy and paste, there we go. So there's the other one right there. Camden says, going to do a phishing simulation for sure. That's excellent. What about others? Analise says, we can increase training and resources, share information more regularly directly with staff, not just when there's an annoying new update. I always say, send the good news, not just the bad news, right? Stay at the forefront. What else do folks think they could do from this conversation? I often tell stories of my mom who was a nurse in several different clinical settings, primary care clinics, that sort of thing, for a long time. And to describe her tech literacy as low would really be the understatement of the century. And I just think like, oh, it would be fantastic if we could get her to use a password manager. So, if you have some folks who are

lovely and wise and all of that, we... Want to get them into a password manager so that they are well equipped. Paige, I will send you that link with not in edit so that you can actually print it here in just a moment while I'm looking for others to share what you might do differently as we wrap up. But hang tight and I will get you that in a way that you can print it.

Jillian And clearly, I didn't mean to still have it in edit mode.

Sarah While you're doing that, Jillian, I want to just call out sort of something that we talked about from the previous two slides, which is the shared like CIO or CISO. I think that is something that the small health center that I worked with could have benefited from, because we didn't really have somebody on staff that had strong skills and leadership in that area. So I think that we probably could have benefited from having like a shared service with other, maybe small clinics or or groups in our area. So.

Jillian Yeah. And I would be really, and again, like this could be a little bit pie in the sky, but I'd be really interested in whether those, those clinics could also share, you know, training services, that sort of thing. I think there's a lot of opportunity for that.

Sarah Yeah, potentially. Because I think some areas, it's a little sticky of like, you don't want to be sending stuff back and forth. That's like obviously PHI or anything like that. But even like proprietary stuff, if that exists as well. But I agree with you, I think that sharing and collaboration could be a good approach for strengthening small organizations in this area.

Jillian Absolutely, absolutely. So please take a moment to complete the evaluation. Put any other questions or thoughts that you have in the chat. It's been great to be in conversation with you all. I think folks have shared some really interesting thoughts. Thank you so much for the kind words. I'm gonna read them for Lisa's benefit. Thanks to all involved for the incredible education and resources that RHNTC has provided to Title X programs for so many years. We love you. Camden says, thank you so for the training. I appreciate it so much. Thank you. Thanks to both of you for sharing so much in the chat and others. Waldyr says, thank you for the great info. Geeky but great. I got you if that's the topic. Thank you. All right. Thanks all so much for being here. Really, really appreciate it and we will see you soon. Bye, everyone.

Lisa Thank you all.