Center for Connected Health Policy
NCTRC October Webinar
Thursday, October 14, 2021
2:00 – 3:00 p.m. ET
Remote CART Captioning

>> Thanks, everyone, for joining today.
Thank you all. We're going to get started here. It is 11:00. Welcome to the latest presentation in the telehealth resource center webinar series.
These webinars are designed to provide timely information to support and guide the development of your telehealth programs.
These are typically presented on the third Thursday of each month.
Located throughout the country, there are 12 telehealth resource centers and 2 national telehealth resource centers.
A few tips before we get started. Your audio has been muted. Please use the Q and A section to ask questions.
Questions will be answered at the end of the presentation or answered in writing following the presentation.
Please note that closed captioning is available and located at the bottom of your screen.
Today's webinar is being recorded and you'll be able to it access it on the NCTRC YouTube channel.
It's my pleasure to introduces today’s webinar and your presenters Jeanne Varner Powell and David Shelley.
Jeanne Varner Powell. In 2020, she left litigation to join MICA as the senior risk management consultant.
She consults directly with insured physicians and practices. Jeanne.
>> Good morning. Thanks, Michael. Ransomware and healthcare can no longer be considered just a tech issue.
There's been a significant increase in the severity, frequency, and scope of these attacks.
As a result, ransomware attacks and other cyber incidents are now creating significant patient safety issue.
A case in paint that you all may have seen in the last few weeks in the news headlines involves a hospital in Alabama.
That hospital suffered a ransomware attack a couple of years ago.
There's a lawsuit file by a patient who came there during the ransomware attack to deliver her baby.
The lawsuit alleges that healthcare providers were unable to access fetal monitoring equipment that was necessary to ensure the safe delivery of the baby.

The lawsuit alleges that as a result the baby was delivered with complications, with injuries and eventually died.
So I'm sure it's no surprise to you when I say that the healthcare setting is really the perfect extortion opportunity for cyber criminals.
If compute systems are disabled hospitals are unable to provide patient care.
Patient data is estimated to be worth 10 to 20 times the value of credit card data in the dark web.
Historically healthcare organizations are easy targets with many weaknesses
Statistics show that health care organizations are less likely to have backups available, less successful in discovering and stopping ransomware attacks and more likely to pay ran some.
Many are using outdated systems that can no longer incorporate the latest security updates.
We have limit information technology budgets and devote more money to speed and information sharing than to data security.
Staff are often under trained on data security measures and there was a spike in remote access during the pandemic.
Remote access is now one of the more frequent entry points for ransomware attacks.
A cyber-attack can make a hospital unable to provide patient care.
The sudden interruption leaves medical professionals susceptible to lawsuits.
Diagnostic errors. Delays in treatment. Though we hear about attacks on hospitals in the news, medical practices and smaller healthcare provides are at risk.
HC3 reports in the first part of this year ransomware criminals targeted medical practices far more than hospitals.
Data breaches are also on the rise.
72 percent of the ransomware incidents tracked by HC3 this year have involved data leeks and in 2020 ransomware was responsible for about 50 percent of all health care data breaches. Data breaches can result in the erosion of patient trust.
You have patients leaving your practice. There can be significant danger to your organization's reputation.
Data breaches can also lead to government compliance investigations which can result in penalties and privacy lawsuits by patients whose data was compromised.
As far as the cost to recover from a ransomware attack, one recent survey of a small to midsize health entity put the price tag at 1.27 million.
Data restoration, rebuilding your computer system if hardware or software is impacted, hiring PR firm or a law firm.
Legal defense costs, lawsuit settlement costs, the price of credit monitoring, lost income is significant due to business interruption and having to cancel patient appointments.
Regulatory fines and penalties that may arise out of a HIPAA compliance investigation.
The next few slides focus on the HIPAA security rule.
In the interest of time I'm going to go quickly through those to give you an overview of its significance.
On the resources page at the end of this slide deck I've included links.
Health care organizations are required to comply with HIPAA. It also requires healthcare professionals to ensure that only those individuals who should have access to E PHI do have access.

Next slide.
The security rule requires entities to perform a comprehensive risk analysis and have a written policy and procedure in place. During audits in 2016 and ’17, OCR found that only 14 percent of health care entities are in substantial compliance with the risk analysis requirements. You need to identify all your PHI, determine and analyze the risks to the confident and integrity of the EPHI. You need to document the analysis and retain copies of the documentation.
HHS has a good security risk analysis tool and I have a link to that on the resources page.
After you conduct a risk analysis, you need to implement security measures to reduce each risk to a reasonable and appropriate level. You need written procedures in place to prevent, detect, contain security violations and policies and procedures in place to guide your risk management activities.
And you need to document each phase of the process and retain the documentation.
During audits, OCR found that 94 percent of entities failed to implement safeguards to reduce the risks it a reasonable level.
OCR does periodically audit health care entities. It investigates an organization any time a data breach is recorded. I'll take this opportunity to recommend to you that if you and your organization are not in compliance with the security rule, you take the steps to get in compliance.
Compliance not only helps you avoid regulatory fines and penalties, but also greatly reduces the risk of a cyber attack. Given the costly ramifications of a cyber attack, it's money went spent to comply with the security rule.
Let's talk about what the security rule requires if a health care organization suffers an attack.
First of all, before an attack ever occurs, and hopefully it never does, the security rule requires you to prepare ahead of time by developing written, reasonable appropriate procedures and response processes.
You need a comprehensive written plan in place that you've tested ahead of time, very important, that will allow you to address and recover from a ransomware attack.
Under HIPAA a security incident is defined as the attempted or successful unauthorized access, use, modification, or destruction of information or interference with the operations of an information system.
The presence of malware is a security incident under the security rule and at the time the entity discovers this incident it must initiate its response procedures. You plan needs mitigate potential harm. This includes incident scope, where it originated, whether it's ongoing or finished and how it occurs. Then responding to the vulnerabilities that permitted the attack, restore loss data and return to business as usual.
You're required to document security incidents, the outcome and all of the steps you take along the way in response to the incident and you need to retain the documentation in case of a later investigation.
In addition, the security rule requires that a healthcare entity have a written contingency plan in place that it will implement in the event of a security incident and you need it have data backup, disaster recovery and emergency mode plans.
Finally, OCH recommends reporting ransomware attacks to the FBI and other law enforcement agency.

Let's talk about breach.
In health care ransomware attacks and data breaches go hand-in-hand. Health care is now the most targeting sector for data breaches, ransomware attacks were responsible for 50 percent of all health care data breaches in 2020.
Under HIPAA, breach is defined as the acquisition, access, and use of PHI in a manner not permitted which compromise security of PHI. You must take an assessment of whether a breach occurred. You are required to document and retain all information considered in the investigation and if you decide no breach occurred, you need to document how you reached that conclusion.
It's important to know that in the event of a ransomware attack, OCR presumes a breach. You can rebut that presumption but first I'd like to outline what HIPAA requires in terms of breach reporting.
In the case of the breach of protecting health care information, the entity must notify each victim within 60 days. If the breach affects 500 or more people, the entity must notify OCR and the media.
Fewer than 500 people, you must report to the OCR within 60 days in the calendar year in which the breach occurred. I'm going to pass over the state data breach discussion. Suffice it to say each state has and more and more states are implementing their own data breach and privacy laws and some states have more stringent laws that actually put further obligations on top of health care providers and other businesses above what HIPAA requires.
It's important if you have a data breach situation to work with your legal team to be aware of the state data breach laws so you can stay in compliance.
I hope you never have to send breach notification letters to patients, but please remember HIPAA dictates the content of these letters.
OCR finds that most breach notification letters don't contain all of the required information.
The letter needs to be written in plain language, provide a brief description of the breach including dates of breach and breach discover date. Describe the types of information involved.
List the steps effected individuals should take.
Describe what you're going to investigate the breach. Include contact information for your practice or organization so people can ask questions.
This may be a toll-free number, email address or postal are dress or website.
You need to send the letter by first class mail and you need to send the letter within 60 days of discovery of the breach.
If you have contact information for ten or more patients that is out of date, you have to provide a substitute form of notice.
You can post a notice on the homepage of your website for at least 90 days or post in a major print or broadcast media.
As I said, you can rebut the presumption of breach. This is not a task a medical practice would take on its own. It's delegated to an IT forensic teams and legal team.
In addition, in the situation where the data is encrypted and remains encrypted, there is no breach but that is a technical determination that you need to delegate to technical and legal experts working on your behalf.

As part of rebutting the breech presumption, it's crucial to conduct an investigation in a way that previews technical forensic evidence that you may be able to use in your rebuttal. You need evidence to support a determination that no breach occurred. You want to show that no breach occurred because then you won't have breach notification obligations. This can save you time, money, and preserve good trust. For this you'll rely on your technical and legal teams. I recommend checking your cyber liability insurance policy.

Once you report a claim, your cyber carrier may assist in selecting a legal and IT team. You should also consider reporting ransomware attacks to your insurance carrier especially since in attacks we're more and more seeing potentially medical negligence types of claims, potentially your medical liability policy may come into play for coverage.

In the interest of time, I'm not going to go through this list of forensic dos and don'ts. But it's a great list of considerations and hopefully the message it sends is that you don't want to forge ahead on your own.

Get a technical and legal team in place that are experienced in ransomware to direct the activities in order to preserve the forensic evidence.

I just want to cover briefly lawsuits and allegations that we're seeing lately arising out of ransomware attacks. In data breaches involving large healthcare systems, banner or this year scripts, we're seeing class action lawsuits being filed. Most of these are alleging violation of state privacy laws, negligence, breach of contract.

Some of these are being dismissed by judges on the basis that the damages are too speculative.

For instance, a case involves envision health care in Nevada. The plaintiff claimed losing time checking financial accounts and answering spam calls, she also alleged stress with dealing with the effects of the breach and worry and anxiety about applying for new credit cards, also concern that damage to her credit worthiness would impact her future ability to obtain credit.

The trial court dismissed the case. It was appealed and reached the 9th circuit. The court held that lost time was not compensable and there was no evidence that her credit had not lost value. There's no information the personal information has lost value or been stolen so the damages claims are too speculative. In a federal lawsuit in 2020 in Pennsylvania, the judge dismissed two claims alleging the attack put the plaintiff at greater risk for identity theft.

Another claim said that the IT systems downside caused a delay in the surgery he need and because of that he continued to miss work and then as a result he lost his employer provided health insurance which forced him to purchase a higher cost insurance. We'll follow that case.

Here is another lawsuit. Electa suffered a ransomware attack which forced it to take its software offline for a period of time. Plaintiffs have filed ail class action lawsuit alleging this down time prevented or delayed treatment for cancer patients nationwide.

Finally, after a ransomware attack in Alabama, that's the one I talked about with the patient who recently filed a wrongful death claim arising out of the loss of her baby, but that are other patients filing lawsuits claiming they were forced to forgo medical treatment.

So some risk reduction strategies. In closing I'd like to stress that you should strongly consider cyber liability insurance. Use the HIPAA security rule compliance to manage

risk and avoid fines, penalties and corrective action plans and carefully vet and select a reputable IT vendor.
I've talked to physicians who thought they had backups in place that would be useable and not subject to ransomware infection that were stored offline if they suffered an attack and when they did, the backups were not available.
You should be checking with your vendor periodically for evidence they're doing what you assume they're doing.
Arrange for cybersecurity training for any employs in your organization.
Again, your cyber and NPL carriers may be able to suggest resources in this area.
Thank you, that's all I have.
>> Thank you very much, Jeanne. Excellent presentation. It's clearly important for health care providers to utilize well-qualified professionals in their cybersecurity programs. Now it's my pleasure to introduce David Shelley.
He loves helping organizations stay current on cutting edge technology that's reliable, secure, and current. A very transparent individual. He is a talented, driven and competent leader. Strong background in technical delivery and customer relations.
Please take it away, David. You're muted. Still not hearing you. We heard you at the beginning of the call, but can't hear you now.
Possibly leave computer audio and rejoin it. There's a leave computer audio setting. Then click that again to join it again.
No. Maybe unplug and replug your headset.
Bear with us everyone. If you have a phone available, if you go to the same menu and click switch to phone audio it will give you a number to call and give you the instructions to connect.
Still not hearing you.
Thanks for your patience as we work through a technical glitch.
>> How about now?
>> Excellent. Thank you.
>> Okay. Very good. Thanks for the time today, thank you, Zoom for messing up my audio.
So if we can go to the next slide, what we're going to focus on today is some deliverables that we've been doing with health care organizations here in town addressing cybercrime incidents.
That's what we do and I do specifically. We manage a few health care organizations, their IT as well as do forensics on where their vulnerabilities are in the system and how to cover those gaps.
This is a rabbit whole of a subject matter of all of the different areas that need to be addressed.
What I'll focus on is key deliverables that we're going into and seeing that organizations aren't addressing.
These are clear things that your internal IT staff can address and implement and address ransomware getting into your environment.
Try to close that gap.
The one thing we tend to see in organizations have multiple directories.
We recommend having a single directory structure that is administering all the devices.
All the devices are connected and have two-factor authentication set up.

Any time a device logs into an application, there should be some form of two-factor associated.
There's a lot of products out there that can facilitate that, it's a matter of addressing it and deploying it system-wide.
Our mindset when it comes to security is building security in layers.
If a consultant says there is this one product that will fill all these holes, they're lying or not knowledgeable in this area.
There's not one single product that will address vulnerabilities in your system.
You have to build your security in different layers in the event of one of them failing.
Because hackers are smarter than your IT folks and smarter than me.
They're constantly moving the needle.
Having a single directory in place where all your devices are authenticating is crucial.
There are a lot of user accounts that the password policy isn't sufficient enough.
They really need to be 12 characters. You're going to see a lot of compliance where they're going to force 12. You'll see uppercase, lowercase, a number, a symbol. Not reusing passwords. What I see in health care organizations is typically 8 and they have to change their password every 6 months, which is not HIPAA compliant.
This is how most breaches happen is old passwords, old directory accounts. Deleting old active directory accounts, making sure that's clean is a huge step in securing your network.
Two-factor authentication.
I guarantee everyone on the call knows what that means. I won't get into that. But for the most part every email platform, most health care organizations have moved to a cloud based structure.
I still see some internal mail systems, but most of them have Office 365 or Gmail. Two-factor is very, very important because most cybercrimes, most ransomware attacks come in through email.
Someone comes in with an email, they click it, you're done.
That's how quick it can happen.
Two-factor on email to ensure that email accounts aren't getting breached and you're not getting an email saying you need to reset your password. All production devices should have two-factor.
Desktops, tablets usually aren't two-factor.
I've only seen that probably in three health care organizations. All the rest don't have it to that layer.
That's extremely important.
Those tablets are very susceptible to breach. Most tablets my guys can hack in 10 minutes.
The tablets that are used in health care aren't really meant to be extremely secure.
They're not built for that.
All remote desktop sessions, most medical applications that organizations leverage are published through RDS or mode desktop or citrus. That's how a lot of breaches have happened in the last year and they've gotten news worthy media attention. There should be a VPN if you're leveraging a public app for your platform.

Also all application leverage, EMR, Dropbox et cetera should had been set up for two-factor if it's client or web based. Box or Dropbox people use it to share information and don't realize how easy it is to hack.
Someone mentioned to me that 2FA is not necessarily that secure because you can basically spoof a sim card. It's difficult to spoof a sim card to get that secondary code. Verizon, ATT have made difficult to get a sim card with an organization. They're making their strides to make it more secure in the space as well.
Next-gen anti-virus managed threat response. You're going to start to see every insurance organization starting next year to get renewed. I've already started to see it this year. They will not renew cybersecurity insurance for organizations unless you have next-gen anti-virus. Means you're replacing your old anti-virus product with another product that addresses specifically ransomware, the crypto locker and all of the different flavors of crypto as well as it ties into a back end network operating center that is constantly checking for abnormal behavior.
Meaning if Michael never logs in at 2:00 a.m. or that specific he device he uses is never logged in at 2:00 a.m. and it does on an odd morning, it's going to create a ticket and watch the behavior on that device.
If it's malicious it is going to kick that device out the network.
They're constantly watching for this type of behavior. The software is coded where if crypto starts to kick off it will stop it at that device before it goes to your file systems or patient data.
That's probably the most important tool in today's climate and it gets overlooked because it's not cheap. You probably don't have it installed unless you're paying $15 to $20 a month per device. To get that MTR, the least amount even with Crowd Strike, SentinelOne, the entry point is around 15 to $17 a month. It's well worth it.
I've installed it in abundance this last year.
Sohos, SentinelOne, Trendmicro will not allow malicious hacking tools that they use and we constantly are scanning for to remove from the networks that we engage with.
Commercial grade firewall.
Most health care organizations that are your hospital systems definitely have very good sound firewalls.
But a lot of the smaller base systems, two to three, clinics, smaller organizations I'm always shocked to walk in there and find a firewall that you can buy off Amazon, at best buy. Those types of devices typically do not have some of the features outlined in this slide that are extremely important.
Some of the things that are required in this -- this is the most important device in your network. It's the gateway. It's the bouncer of your network. It needs to have intrusion protection service which is constantly scanning for threats. It's going to alert you when you get a lot of log in requests. Like Jeanne said is a lot of work is being done remotely. This particular device is going to capture all of that traffic and catch that weird activity before it touches your systems. Having the right products set up are going to stop a lot of these mishaps before happening. Geofencing is also a great feature. If you know all of your clients are in a certain area of the world, lock it to that.
Unless you have patients and work that is going to be done from those areas, lock the users down so they can't ping you from those geographical areas.

Web filtering is also a huge deliverable that typically gets over looked in terms of severity level. I lockdown everything and then allow access.
I'm more lock everything down and then provide access, work with the organization, find out what sites they need to go to because most people are coming in from easily users just browsing the internet, going to sites they shouldn't go to.
Correct spam service. Most crypto comes in through email, unfortunately. Having the correct spam service that is doing features like silver lists, basically your email server saying are you a legitimate source. That cuts down on a lot of attempts.
There's a lot of great products wrapped around spam services. I have them listed here before. These are all great products that do this feature set.
They also have their brand of what I call target threat protection. Any links that come within an email and even images that if you click they have a hyperlink associated. Every link is opened at one of these services first to validate it's a good link with no malicious consent and then it will open in your browser., that that's going to cut down on a lot of malicious attempts. This is typically not installed. To hit a link in your email and launch into your explorer, it might take 3 to 4 seconds as opposed to one. Most doctors and admin staff don't want to wait the 2 to 3 seconds, but the value of waiting, there's so much more value in having that feature set associated in my humble view.
It also deals with impersonations. This is a common thing within organizations. The CEO will email someone and it's not him. These services will stop that process from happening, whether it's internal or external.
Point in time backup solution. In the last few years we've got a lot of media attention around crypto. These health care organizations didn't have viable backup solutions. It's not because they wanted to find the data that was stolen. I could go on the dark web and buy patient data.
It got media attention because the organizations were being held for random but they also didn't have viable backups. Backups and having the right vulnerability software are the two most important attributes in my view.
Point in time means that if ransomware happened 10 hours ago and if only affected a certain portion within the network and the IT got notice of it this hour, they can literally go to 11 hours ago and restore all that data back down within two to 4 hours.
And any back up system should be set up and architected in a way where you could push down 60 to 70 percent of your data in 2 to 4 hours. If you back up system can't facilitate that timeline, it's not the right back up solution.
That should be rebuilt.
Point in time basically means you're not backing up once a day. Most healthcare systems do twice a day. I recommend every two or four hours you take a snapshot.
Even if you do all of these things you can still get ransomware. You have to plan for the worst. The one thing they can't touch is your back up. Even if you get crypto, it's not touching your back up data. Your back up repository should also replicate off site.
If you're following HIPAA, your back up data is off site.
Typically, that backup system has direct access to the third party site that's replicating the data. That's a big no-no.
The onsite system should have no conduit that will bounce to the server. It needs to be in its own separate network.

You have to treat it for worst case scenario. We're segregating back up platforms whether it's in the cloud, in a secondary location.
There are a lot of great products that will facilitate what I discussed. Quest has a product. Veeam has a great product. Vulnerability scans, so Jeanne mentioned it's extremely important to work with an IT organization that can come in periodically to do vulnerability scans and work with your IT department to specify we found these vulnerabilities. There is a cost associated. But that should be done every quarter.
As well as user training. There's a lot of great products where you can send emails to your staff that are phishing or crypto or that are fake. If Jeanne opens it, not only is IT going to know about it, they're going to tell Jeanne what she did and what to do next time.
These are the preventive natures you're going to start to see HIPAA push.
They're going to say you have to do these training activities because systems aren't locked down the way they should be. I think HIPAA and OCR are aware of that.
They're going to cover their bases.
Find an IT firm or find the right software. There's a lot of great software out there. We use rapid fire and get your IT department to run these types of activities and to true up these vulnerabilities, because the vulnerabilities you fixed 6 months ago, there's more now. Unless you're constantly on top of it, you can go 2 years without checking and all of the sudden you have a boat load of vulnerabilities and then the cost point to fix it is going to be substantially higher.
So basically that's everything I want that talk about regarding ransomware. I don't know if there's a Q and A session, but we can address questions from the user group.
>> Thank you, David. That was an excellent presentation. I really enjoyed your insights into the current attacks on health care and what is needed to prevent those from succeeded. Ben Franklin said, “An ounce of prevention is worth a pound of cure.”
I still don't see any questions, but people in the audience, we have about 7 minutes left in the hour. Please feel free to chat in or put a question in the Q and A. I have a question for Jeanne.
What are the responsibilities of a business associate when it comes to complying with cybersecurity regulations and risks?
Maybe a hospital system, you know, contracts out some of their billing or other work, what sort of responsibilities do those contractors have?
>> Business associates are also covered under HIPAA, so they basically have the same responsibilities that you as a health care entity have.
It's important when you're contracting with your business associates to ensure by periodically checking that they are in compliance as well.
Typically, when there's -- if they are the ones maybe maintaining records and the data breach situation is on their end, while let's say maybe they are the tech vender for your EHR, you may end up notifying your patients but you can make contractual arrangements to adjust for that.
But they will have liability as well.
I think that 1 case I talked about with Electa there's allegations where the allegation against the medical practices and providers who used the company failed to adequately vet that vendor and should have vetted them better to safeguard their patient's data.

You need to be in close contact with your business associates and make sure they're doing the things they need to do.
But HIPAA applies to them and there are business associate types of entities that have been investigated by OCR.
>> Thank you. Still not seeing any other questions. David, what do you recommend that an organization do when they believe that they may have been compromised? Should they turn systems off, disconnect from networks?
>> Unfortunately, there isn't an easy process there. Primarily because if you feel you've been breached, you just can't disconnect the device or the user account. For example, 2 weeks ago an organization got breached and we got called in. It took three guys 4 days to get them out.
Just because they used software that's extremely intelligent. It's like a spider web, I can wipe it off 500 machines and miss one and then it replicates it back to everything.
So it's like whack-a-mole, unfortunately. If you feel that you've been breached, you need to rely on people that have not done this once or twice, someone that's done this 100 times in the last 2 years and they need to come in with their tool sets and knock it out quickly.
Some of these tools that we have are tools that my team got off the dark web. And some of the tools I've spent a lot of money on.
My point being, having your internal IT team figure it out, typically that happens for a month and then they call someone like our organization because they can't get rid of it.
That's my recommendation. There's no silver bullet of disconnect the infected device off the network. 99 percent of the time it's already somewhere else in the network. Most breaches have been in there for three months and you didn't know about it.
Then IT becomes aware of it.
And they're shuffling to get them out.
>> Thank you very much. Well, I don't see any questions from the audience, but thank you very much for attending, everyone.
We do value your opinion greatly and ask that you take a few minutes and complete the online survey. That will help us to improve our webinars in the future and help to address topics that are of interest to you.
Thank you all very much.