NCHICA Podcast featuring David Holtzman of CynergisTek

Posted 4/15/2020

Welcome to the Healthcare IT Trends Buzz. This podcast is a production of NCHICA, the North Carolina Healthcare Information and Communications Alliance. NCHICA is a nonprofit consortium dedicated to accelerating the transformation of the U S healthcare system through the effective use of information technology, informatics and analytics. My name is Janet Kennedy and I'm also the host of the Get Social Health podcast. On this episode we have an NCHICA member profile. We're going to be interviewing David Holtzman. He's an Executive Advisor for CynergisTek and he's also a subject matter expert in health information privacy policy and compliance issues involving HIPAA privacy, security and breach notification rules. Welcome to the podcast, David.

Well, thank you very much, Janet. It's a pleasure to be with you today.

The last time we spoke was in 2017 as you were preparing to give a session at the NCHICA annual conference on how to prepare for a HIPAA audit or compliance review. Well, a lot has happened since 2017 and honestly the last 90 days have been pretty amazing. I imagine that you've been greatly impacted in your area by COVID-19.

Yes, and I hope that everyone listening to this podcast is safe and healthy and safe in their home.

That is excellent advice and sadly, while this podcast may last for a few months, we may also still be encouraging people to be very cautious and be much more aware of how they're interacting with each other for quite a while.

Yes, that's probably the unfortunate reality as we speak today in early April, the public health experts are forecasting that this current situation may last well into the summer.

You know, this has been a huge strain on absolutely every aspect of healthcare from top to bottom. And one of the most interesting things that I have witnessed is how our government has responded and loosened up a lot of regulations regarding patient privacy. So I'm very curious to know how you think that the HIPAA privacy and security standards have been impacted by the federal government's response to the COVID-19 pandemic.

You know that's a great question, Janet, and we've seen a lot of activity here in late March and early April. But let's start from the standpoint that most HIPAA standards are not relaxed during a period of health emergency. Covered entities and business associates must still implement reasonable safeguards to protect protected health information from unauthorized disclosures. And PHI may only be used or disclosed in certain circumstances when needed for patient care or other important business and public health purposes. So the bottom line is that HIPAA covered entities and business associates must safeguard the confidentiality, integrity and availability of patient information that's created, maintained or transmitted through an electronic device or stored on an information system.

I, as you know, am a social media person and certainly getting very involved in supporting the face mask production for healthcare organizations. And we are seeing a lot of photos coming from healthcare organizations. Are you concerned about that?

Yes, there is a great concern, but you know it's important to remember that the Privacy Rule permits covered entities to disclose protected health information without authorization in a period of a public health emergency. So it's important to remember that PHI can always be shared with the patient, or to another health care provider if necessary to treat the patient, or if it would help treat a different patient to a public health authority, and that is a defined term in the Privacy Rule, or to persons at risk for contracting or spreading a disease or condition when it's authorized by law. So for example, for contact tracing of an infected person in their community with family, friends and caregivers involved in caring for that patient or when there is an imminent threat to public health and safety. And as always, PHI can be shared with business associates or contractors or vendors even if they're volunteers to help in the treatment of the individual or in the case of creating a customized face mask so that you're able to create that type of appliance to help in the person's treatment.

Another important thing to remember is that health information can be shared with first responders and law enforcement. So the HIPAA Privacy Rule allows for disclosure of PHI when the notifications required by law or to notify the public health authority or a first responder to prevent or control the spread of disease or when first responders may be at risk of infection as well as to prevent or lessen a serious or imminent threat to the health or safety of that individual. But it's important to remember that the minimum necessary standard applies to these disclosures, especially to first responders and law enforcement. So there's a resource that's available on OCR's website for when protected health information may be disclosed in a public health emergency. It's a workflow in format and I urge folks to go to OCR's website, https://www.hhs.gov/hipaa/, and look under public health emergency and contingency planning.

Well, actually we'll also make sure that it's on the NCHICA website attached to this podcast.

That's super.

Well, tell me about telehealth. This has certainly been very, very exciting hearing about all the ability to open up the floodgates and finally let people start to speak to clinicians via video apps. On the other hand, there aren't very many video apps that I feel certainly secure in sharing some of that kind of information. So what's your take on how the changes that we've seen and how healthcare providers can use commonly available telehealth and video conferencing services?

You know, it's a double-edged sword, Janet. You're absolutely right. On the one hand, it's important to remember that these telehealth applications and technologies, we depend upon them to ensure the confidentiality and cybersecurity of the data that they're creating and maintaining. But by the same token, we're in an unprecedented period where to limit the spread of the Coronavirus, HHS in late March loosened the requirements for using telehealth so that commonly available texting and video conferencing technologies could be used without fear of applying the HIPAA privacy, security or breach notification requirements. So OCR is using its enforcement discretion during a health emergency. Healthcare providers, but not health plans themselves, healthcare providers can use commonly available messaging and video conferencing applications like FaceTime, Google Hangouts, video, and WhatsApp. It applies to any healthcare treatment encounter and is not limited to telehealth services that are provided only for Coronavirus assessment or testing.

However, it's important to remember that the enforcement discretion or the ability to use these technologies bars the use of public-facing video technologies, technologies that broadcast video publicly like Facebook Live, Twitch or TikTok, just to name a few examples. And as always, it's important to let

patients know of the risks of using unsecured technologies. One of the other considerations is: what are the best practices that healthcare providers should be using to safeguard ePHI in this era of free use of common technologies? So we should use communication methods including smart phones, video conferencing, and other technology platforms that safeguard the confidentiality, integrity and availability of data, which generally means that they be secure and encrypted. Providers should still attempt to have business associate agreements in place with technology vendors prior to providing PHI or patient care via video conference. That is your assurance that the technologies that you're using are safe and secure, and choose telehealth vendors that can demonstrate they have effective risk-based information security programs in place. Even in this period where there is some regulatory flexibility in allowing for the common use of technology tools, it's always best to use the most secure and most reliable resources out there to both protect the confidentiality of your patients and also to assure the cybersecurity of your own information systems.

Now, does that mean that the meeting with the clinician always should be initiated by the clinician and not the other way around?

In order to assure that the technology is as secure as possible, the clinician should initiate the encounter. And another important reminder is if you're recording the encounter session, make sure that you've taken steps to rename the file and to store it in a secure location. Don't rely on the video conference vendor to use its default naming convention because as we've seen in a number of examples, those default naming conventions may not always be secure and they could be on un-encrypted or open websites that will be available to anyone who is familiar with the naming convention.

Do you think that these encounters should be or should not be recorded?

That's a very interesting question. The fact that OCR has loosened its enforcement discretion on what technologies are used does not change the requirements of state licensing organizations that require some telehealth encounters be made a part of the patient's permanent medical record. In addition, the patient may have their rights under state law or HIPAA to get access to a copy of their encounter. So my advice is that if you're going to record the encounter you should not fear doing so as long as you can securely maintain any copy that you're creating.

Well they used to talk about when social media came to healthcare that it was the wild, wild West, but I've never seen anything like the last six weeks or so regarding the Coronavirus impact and how people are talking about it, how people are sharing information, correct, incorrect, etc. And I am really curious to know about enforcement. For instance, tell you what, I'm going to ask you a couple of scenarios when we finish, but let's start with the basics. What is the situation with penalties? Is it a free get out of jail card right now?

During this period of health emergency, the Office for Civil Rights has said that it will not levy any fine or penalty against a healthcare provider who uses telehealth technologies, whether they be text messaging applications or video conferencing tools, in good faith in treatment encounters. The devil in the detail here is what is good faith? Good faith is using technologies that are not public-facing. In other words, technologies that establish a connection that can only be viewed by the healthcare provider and the patient. So whether that be a text messaging technology in which there's direct messaging between the healthcare provider and the patient and no one else can view it, or a video conferencing technology that does not rebroadcast the session into a live viewing space. So for example, if you're using a smart phone

technology like FaceTime or Google Hangout, chat or WhatsApp, you can be assured that those types of transmissions are private only between the healthcare provider and the patient.

The non-good faith or things that are not covered by OCR is enforcement discretion. In other words, areas in which there could be penalties still levied is when you're using technologies that broadcast the session so that they can be viewed by others, and examples of those technologies are Facebook Messenger Live and TikTok. But the idea is that if you're using a private session, then you're safe. OCR has said they will carefully review any complaints or compliance review that they initiate to ensure that the healthcare provider used good faith and would only apply penalties where good faith was not evident. Other examples of where good faith is not being exercised is when the session is being used for another purpose. So for example, it's being sold to a third party or it's being used for marketing purposes or it's being shared with a data analytics provider like a Google or Facebook. Other examples of bad faith are if you are not licensed to be a healthcare provider or you're providing healthcare services that are beyond your professional expertise. If you have no state license to be providing a healthcare service and providing the telehealth service will not be permitted or covered under the healthcare exception.

Now, this is about protected health information. If a patient, however, approves and say they're doing an interview with, what did it feel like when you were in respiratory distress? If they have agreed to it and theoretically signed an agreement that they are willing to be in that interview, we're all good, right?

Yes. At any time for purposes other than treatment, payment or healthcare operations, a patient's authorization is required. So for example, if you are conducting an interview between a healthcare provider and a patient to create a podcast, the healthcare provider would be required to obtain the authorization of the patient in order to be able to discuss their protected health information. But if a patient volunteers their own information and it's not related to a treatment encounter or other situation that's related to their healthcare, then that is outside of the protections of the HIPAA Privacy Rule.

What I have seen, which is a little bit frightening to me, are the clinicians who've posted in Facebook, you know, it was an awful day. We lost three people. We lost a 25 year old and they're giving out a little bit of information. They're not releasing names, but in theory, if people knew that it was their brother, cousin, uncle, who had gone into that hospital, that might be releasing information or am I getting a little too in the weeds here?

Those are important concerns. If an individual believes that a healthcare provider disclosed identifiable information about them or a loved one, they should file a complaint with the Office for Civil Rights. The Office for Civil Rights will conduct a thorough investigation of the facts and circumstances and will, when appropriate, conduct an enforcement action involving a healthcare provider. Sometimes, you know, the healthcare provider will make an inadvertent disclosure and OCR takes a measured response. Oftentimes, so long as the healthcare provider recognizes that they disclosed information and takes corrective action voluntarily to ensure that there is not a another incident like that, then oftentimes the matter is resolved informally without imposition of a fine or penalty. But certainly if an individual believes that their health information has been disclosed, the way to make things better and to ensure that it doesn't happen again is to make your concerns known to the healthcare provider. And if that doesn't get the response that you feel is appropriate, file a complaint with the Office for Civil Rights.

As we look at the advance of COVID-19 and the changes that are happening literally daily, what is your advice to healthcare organizations in keeping up with the legalities of managing PHI in a health crisis?

So I often shy away from using the word legality because what organizations are really trying to understand is how can they comply with the requirements of the HIPAA Privacy and Security Rules, any state law requirements as well as to maintain the trust and confidence of their patients and their family members. And so it's important to use the OCR's website as a resource. So it's again https://www.hhs.gov/hipaa/ and on the OCR webpage they have a special section devoted specifically to developments and changes related as a result of the current COVID-19 pandemic. There's also a large wealth of materials there designed for healthcare professionals to help them understand the requirements and guidelines of the HIPAA Privacy and Security Rules, a number of FAQs and scenarios that will help them simplify and understand what the sometimes complex and changing requirements are on a day-to-day basis.

Well, David, I very much appreciate your being part of the Healthcare IT Trends Buzz. This is such important information that will be made available to everybody very quickly because this is a very scary time, but I think it's also important to know that people are thinking through how we need to be reacting to this on all levels and I very much appreciate your insights here.

Well, thank you Janet and thanks NCHICA for allowing this important information to be shared with its membership.

You've been listening to the Healthcare IT Trends Buzz. This podcast is a production of NCHICA, the North Carolina Healthcare Information and Communications Alliance. Thanks for listening, and please subscribe to the podcast so you can hear future episodes. Thank you for joining me, David.

Thank you Janet, have a great day.