Protecting physicians and hospitals from emerging cyberthreats

Watch the AMA's daily COVID-19 update, with insights from AMA leaders and experts about the pandemic.

Featured topic and speakers

In today’s COVID-19 update, AMA discusses emerging cyber threats and what hospitals and physicians can do to protect themselves during the pandemic.

Learn more at the AMA COVID-19 resource center.

Speakers

- Laura Hoffman, JD, assistant director, Federal Affairs, AMA

Transcript

Unger: Hello, this is the American Medical Association's COVID-19 Update. Today we're talking about emerging cyber threats and what hospitals and physicians can do to protect themselves during the pandemic. I'm joined today by Laura Hoffman, the AMA's assistant director of federal affairs in Washington, DC. I'm Todd Unger, AMA's chief experience officer in Chicago. Laura, we've heard talk of some new cyber threats against hospitals recently. What's going on, and is there a cause for concern?

Hoffman: Yeah, lots going on and definitely cause for some concern, but we'll all remain calm and carry on, right? But definitely things that we want physicians to be thinking about regardless of where

they practice. We've talked previously, Todd, about the increasing reliance on telehealth and how more patients are receiving care from home using different telehealth platforms, which has been, of course, a wonderful way for us to promote social distancing and preserving PPE.

But at the same time, what is good for the health care system and patients presents an opportunity, unfortunately, for cyber criminals. So, they see this now as an opportunity to perhaps exploit these increased use of telehealth systems and the fact that people are working in an environment that they may be less familiar with, and they are going to town in terms of trying to infiltrate to different systems that we've seen.

In the beginning we saw a lot of attacks on phishing and ransomware. Having people click on links for additional PPE that they might be trying to find, which in fact actually would then infect computers and systems. But now we, just in the last couple of weeks, have received some very, very urgent threat notifications from the FBI, the Federal Bureau of Investigation, as well as the cybersecurity infrastructure and security agency known as SISA. And they put out multiple joint statements warning the health care community specifically about impending threats, ramping up cyber-attacks and cyber-criminal activity, and letting folks know that basically the health care sector needs to pay a lot of attention because they are specifically being targeted right now.

Unger: Well, as if the pandemic was not bad enough, it's just yet another instance of where an issue existed before has been made worse by COVID-19. Can you give us any details on what those imminent cybercrime threats might entail and potential effects?

Hoffman: Sure. One of the biggest threats that we've seen recently actually is called the Ryuk ransomware. It's a type of ransomware—it's a little strange—it's almost ransomware as a service where a company designs really good malicious software and then puts it out there into the internet space where pretty much anyone can pick it up and use it as they wish. So, because of the design of that ransomware, we're seeing a lot of insider threats, unfortunately, where folks may recognize that their systems aren't patched as strongly as they should be or completely as they should be, and they're able to just insert this software right into some unsecured systems. One of the biggest examples we've actually seen recently is with the UHS health care system where computers were infected, and many practices had to shut down. Hospital systems where without their EHR for some time, many days.

One thing that is important to remember when these kinds of attacks come is that it's not just something that happens in a back room where the IT staff then gets busy to work and trying to fix the ransomware that has infected the system. It really is a system-wide impact when your systems are shut down. You can't pull up distinct patient records to learn what medications they're on or even what their diagnoses are. You aren't able to see new patients, which often leads to, especially in hospitals, often leads to redirecting patients to different facilities. In fact, recently, I believe it was in Germany, one of the infected hospital systems had to redirect a patient to a hospital that was 20 minutes away,

and unfortunately that patient passed away during that time. And so, this was attributed to that.

Unger: So this is a real threat to patient safety.

Hoffman: Exactly.

Unger: And also, I'm assuming, puts patient information at risk?

Hoffman: Exactly. It's a business continuity issue. It's a patient safety issue. We've even heard reports now that instead of hospitals being approached by ransomwares to receive money to get the information back, sometimes now folks are actually going to patients and saying, "We've locked down your information. We know that you have sensitive mental health information, for example, that you might not want to get out. So you, individual patient, now need to pay us to not release your records more broadly." So, it really is impacting hospitals, practices and patients all the way down the line.

Unger: Wow. Would you say that hospitals and physician practices are more susceptible to these types of threats during a pandemic?

Hoffman: Yeah. I mean, it's as you mentioned earlier, it's always a risk and always something that hospitals and small practices alike should be on the lookout for. But in the pandemic, we rightfully have a lot of resources focused on caring for patients with COVID. So you've got a lot of additional personnel maybe working in different areas of the hospital that they aren't accustomed to, maybe their access controls have had to change in terms of who's allowed out into what portions of the electronic health records, and that can contribute to insider threats as well. Then again, frankly, we've got people continuing to work from home and continuing to receive treatment from home. So the landscape of the vulnerabilities and entry points during the pandemic are increased as compared to a regular health care system where a lot of the care is delivered inside your secure clinic or hospital.

We've now spread out a lot of those technology endpoints, which just provide additional opportunities for cyber attackers to get in. Because in the big systems, yeah, you might hit a big payload with a lot of data, but they may be more secure. Whereas in a smaller practice or a physician working from home, maybe less data, but they may not have the same kinds of robust cybersecurity protections in place, and so it's easier to infiltrate that network and maybe link it to a larger network.

Unger: So this is obviously a very big problem. What should hospitals and physician practices be doing now to protect themselves and their information?

Hoffman: Yes, definitely not too late to take action. One very basic thing to do is check that your software is up to date. Make sure that you've done any patching that you need to, whether it's on a Windows operating system, whether it is your browsers that you just want to make sure are continually being updated so that they address those latest security vulnerabilities. Those are really easy, simple

things that you can do very quickly.

Some hospitals have taken, I'm not recommending this. Some hospitals have taken the step of actually not allowing personal email to be used and have just shut down all of their email systems overall. That is a more dramatic step, but it just goes to show you that a lot of the vulnerability comes in through emails. One thing to consider is giving all of your employees a really serious refresher about the kinds of links they should be clicking on when they review their emails inside the hospital system. Maybe have everybody change their passwords more frequently, make the requirements more complex. I know it just adds one more thing for everybody to remember, but you can use password managers to help with that and come up with complex passwords that you don't need to actually remember every time.

Similarly, you can think about turning on multi-factor authentication so that if someone else tries to log into your account using your credentials that isn't you, you would be notified, for example, on your smartphone or a different email address and have to give permission for that person to actually enter into your account. So very low-hanging fruit steps that people can take to make a big difference.

Unger: Well, you mentioned telehealth upfront and it's one of the reasons this has picked up. Will any of the mitigation measures that you talked about or cyber threats start to affect the use of telehealth or the patient experience in the near future?

Hoffman: Yeah, well, I think it kind of is a little bit, and not necessarily negatively at this point. But for example, a recent survey just came out showing that folks of all ages, especially Gen X and Millennials are really interested in continuing to use telehealth. We know that the use overall has skyrocketed over the last six or seven months. But this same article flagged that, in fact, attacks on telehealth have increased 117% just over this time.

Unger: Wow.

Hoffman: It says that that is for a good reason because, again, we see these expanded vulnerability endpoints, people who are practicing in settings they're not used to. So, while on one hand we have folks saying that they definitely want to continue to use telehealth, they are simultaneously expressing that they are very nervous about breaches of their health care information, especially mental health and anything having to do with their sexual health. They are worried that that information may get out.

So honestly, if we want to keep the utilization rates of telehealth high, we want people to feel more increasingly comfortable using this as a mechanism to receive care and again, promote social distancing and try to keep the inpatient setting for folks with COVID. It really, really behooves all of us to make sure that we're using platforms that keep information protected and secure and help patients to feel comfortable to continue to use these platforms.

One other thing I would say, you asked about during the pandemic, is there a heightened risk? We talked about that, but one other thing I would point out too is just on the regulatory space, there are also a lot of regulations that are starting to go into effect over the next year or two having to do with information blocking, where practices are going to need to start using what are called APIs, which allow greater access to information and flow between systems. They're going to need to be upgrading their technology to a new certified EHR technology. This'll happen on a rolling basis over the next couple of years, but there are also increasing reports of these APIs being very vulnerable to cyber-attacks because they may be very close to the surface, essentially, of the line between where technology is secured and where it isn't. That's not an incredibly technical description, but basically there's an increased vulnerability there as well. So, as more practices start to update their technology in ways they are required to by Federal regulation, that brings an additional risk of cyber-attack that that will be novel to the industry.

Unger: Yeah, so any of those kinds of integrations, which are probably increasing in today's health care space, add vulnerability to it. We're in the middle of another surge. Hospitals are already overwhelmed and bandwidth, obviously, and fatigue probably have an impact here. What resources are there to help hospitals and practices during this time?

Hoffman: Well, there are a bunch, fortunately, and the AMA has put out a couple of them. We have some existing resources pre-COVID that are still available on our website that give practices some, again, very easy to implement, high level tools that, as I mentioned before, you already know, patching, updating software, having strong passwords, the checklist that you can think about in terms of what makes a good, strong system. At the beginning of the pandemic, we put out a special publication in conjunction with the American Hospital Association, and that was focused specifically on practices who are working from home right now. So, those who are doing mostly telehealth work, the kinds of things that you might want to think about as you practice from home.

I'd encourage folks to check that out and that's on our website. Then we followed up that publication with the AHA with a second publication, a technology considerations for the rest of 2020 now that we're seven, eight months in, and again, folks are, they may have set up VPNs, virtual private networks or disseminated laptops and iPads to a whole variety of folks. Maybe now it's time to take a little bit of stock in the time that you can of where those platforms are, who has control over them, how are they being accessed, how are they being used? That resource kind of walks you through some of the considerations to think about there.

Then beyond what the AMA has, would definitely encourage folks to check out the resources made available by the Health Sector Coordinating Council's Cyber Security Working Group. It's a mouthful, but they have really, really excellent guidance that is scaled for all practice sizes. They have a specific task force that is aimed just at small practices that, again, is really easy to understand and scalable. I'd encourage folks to check out their website as well.

Unger: Well, last question. What should physicians watch out for to indicate that they might be at risk here and what do they do if they suspect they've been a victim of cybercrime?

Hoffman: Right. I mean, things you're going to want to watch out for, of course, are the things we all hear about regardless of where you work. Being very careful about suspicious emails, making sure that you know what links you're clicking on. If you get an email from someone and you're not really sure that it's legit, when in doubt, throw it out, delete it. You can always call or send a new email to that person to check whether it's a legitimate communication. So be looking for that kind of thing. And then if you suspect that access permissions have changed, if you're seeing in your audit that folks are in areas of the EHR that maybe they aren't usually allowed to be in or supposed to be in, there could be an explanation. Like I said, a lot of folks are working in different departments of hospitals, for example, than they normally do. But that might also just be a sign that you should check in and make sure that everything is legitimate about that altered access.

Then in terms of who to reach out to. Many years ago, during the WannaCry ransomware, the cyber-attack that was one of our first really big attacks in health care in this country, the Office for Civil Rights, the FBI, a bunch of Federal agencies put out some really good resources for people. The FBI is still always a really great stop because... A good starting point, I should say. Letting them know that this threat exists helps them to also communicate internally in the Federal government with our national security folks and others who are able to better then trace where the threat is coming from, get out information to the community overall.

We know that some health care providers are really hesitant to report these kinds of attacks because they're nervous that it may be considered a breach under HIPAA. And that may be the case, but ultimately, physicians, health care systems should be thinking about the overall threat to the health care system, and again, these patient safety issues and making sure that that information sharing is a priority is honestly really critical during times like these. So, you may wind up needing to talk to the Office for Civil Rights, but they also have a great checklist of who you should reach out to within the FBI and the different agencies, and then the steps you should start taking within your own organization to try to rectify and mitigate some of the effects of the cyber-attack.

Unger: Well, thank you so much, Laura, for giving us your perspective and the information on this. It sounds like it's a huge problem, and unfortunately, one that we have to deal with on top of the pandemic itself.

That's it for today's COVID-19 Update. We'll be back soon with another segment. For resources on COVID-19 and on cybersecurity that Laura talked about, go to ama-assn.org/covid-19. Thanks for joining us and please take care.
