Ransomware Attack and Hospital Downtime Issues

By: Philip Hammarberg and Terence Russo

Philip Hammarberg: Welcome to the Garfunkel Wild Health Care IT Podcast. My name is Philip Hammarberg, and I am a Senior Attorney with Garfunkel Wild. I'm here with Terence Russo, a Partner and the Chair of the firm's Health Care Information Technology Group.

Philip Hammarberg: On today's podcast, we have a special guest. We will be having a discussion with a physician that works at a hospital who recently suffered from a ransomware attack that had significant downtime earlier this year.

Philip Hammarberg: It should be noted that the hospital system in question is not a client of Garfunkel Wild.

Philip Hammarberg: Now without further ado, let's begin. So you are a physician at a hospital that suffered a downtime and ransomware attack, right?

Doctor Correct

Philip Hammarberg: Was there any notice when this happened? Was it something that was really spontaneous? How did you initially find out about it?

Doctor What happened was a spontaneous attack at a really inconvenient time, meaning it was around a holiday and of course a lot of the staff and IT people, and physicians and nurses and so forth, were off for the day and came back on the Monday and found out that nothing was working. So we started getting a clash of texts and phone calls saying that the system was down. And patients were cancelled and so forth and so forth. It happened very abruptly.

Philip Hammarberg: Ok – and when you say nothing was working. Were clinical systems down or payroll or what was happening?

Doctor Early on, it was the EMR system apparently was down. But with that also the WiFi system and anything that connects to the WiFi, for example the fax machine,

badges, things like that, nothing seemed to be working. So the first several hours to the first several days you were finding new things that were happening and you had no idea that that could be involved. But ultimately lead to lots of other things like payroll, payroll delays. And anything you can imagine that is outside of the medical surgical realm that got impacted as well quite severely.

Terence Russo Wow. So Doctor, this is Terence Russo. So, Doctor, unfortunately this has been happening more and more of our clients, our health systems. For some reason bad actors seem to like going after hospitals. So it sounds like the EMR system was down but then it spread to other applications – anything that connected through the network, the WiFi network. I mean payroll is generally different solution than your EHR, so this was fairly widespread downtime. How long did it last approximately?

Doctor Yes, it definitely was a downtime. I don't know the specifics on what exactly was attacked and some of it may have been you know "to prevent further collateral damage we're going to shut this off, we are trying to figure out where the source came", that may have been part of the problem in regards to some of the spillover. But it lasted at least three weeks or so and here and there still does a little sputtering, I call them little aftershocks, you know after the earthquake you get the after earthquake type of effect. So that's kind of where we are at at the moment.

Terence Russo So it's still not perfectly stable. You are getting these aftershocks, these tremors.

Doctor Yea.

Terence Russo So I assume, not only did you have to, I'm assuming you had to probably reschedule patient procedures and maybe the ER. Was the ER affected? How did this affect patient care? Because I kind of want to approach patient care then morale. I can imagine payroll affects morale.

Doctor Yea for sure.

Terence Russo But how was it for patient care? Were procedures rescheduled? Postponed? How did you deal with that?

Doctor Yea, so very good question. So like I mentioned I show up to my surgeries on a Monday and early that Monday a barrage of stuff starts going out about this is and that and so forth, so of course I had four surgeries that day that we couldn't do because we don't even know who is on the schedule, we don't even know who is supposed to be there. The patients didn't get called the day before because there is a lot of stuff that goes through that so those got cancelled. And that first week every single surgery that was an elective basis got cancelled.

Doctor Anything through the ER, well of course they were using the EMHR, so patients would still come in, but everything had to and transition to hand charts, meaning like hand delivery of papers, hand delivery of stuff, waiting for results and hand written – it just really brought us back thirty years in the scheme of electronic

medical records down to note taking and trying to find out who is actually in front of you, is this a patient – we don't have any old records, we don't have any EKGs, we don't have any information about this patient because it is all in the system. So if anything outside the system, you cannot access that you have to start from scratch so it was really hectic for everyone, especially the nurses who spent most of their time trying to track stuff down, and do this and record this and so forth, so very challenging.

Terence Russo I like your calm, saying it was challenging and hectic are probably putting it mildly.

Doctor Haha yea.

Terence Russo We have seen some other clients who have experienced this. You have no allergies, contraindications, all sorts of things you have got to just ask if you don't have a backup. I guess it's funny, because health systems are supposed to have backups and contingency plans and sometimes they are even supposed to practice this. To be down for a couple weeks is very long – I have seen a lot of clients go down three days, five days… but for several weeks… so even though you had probably done some practice before, it sounded like it was a bit of a scramble when it actually happened. If I am understanding you correctly, you didn't even have any advanced notice. It was "I'm here Monday and now I'm not - now I'm canceling procedures that day, day of." It was really, sounded like not a lot of communication. Because what I want to kind of approach Doctor, with your help, is how could other hospitals somehow make it better? It's going to be a horrible experience no matter what. But maybe if there is more communication or backup practices, do you have any kind of takeaways on how you could've maybe mitigated this horrible experience?

Doctor Well let's just imagine for example that the phone system went out in all of the United States and how could you get access to anyone other than within walking distance or maybe driving distance to you, I mean that's how it was. So for us, a bunch of texts started coming through and we ended up going through a secure kind of WhatsApp type, not WhatsApp, but a type of chat function like that where essentially we found everybody, we put them in there and we started talking running things and so they were giving updates via that way so at least the physicians had some sort of update, but I think in the future, communication is definitely going to be key because not everybody checks their email and if your computer is logged into the hospital, you can't get on WiFi anymore, so on and so forth, so communication is going to be key. How do you communicate the problem? That is going to be high on there. But of course everyone is going to say well prevention is worth one ounce, or prevention is worth one ounce of cure, right, so the system got fixed, it got better but how can we prevent this in the future? And I don't know the answer to that because I don't know exactly what the source was. Did it come in through an email or did it come in through to someone's personal computer getting hacked on the system, or did it come in through a vendor? There's so many things that are hush hush right now in terms of what happened. I can just tell you that currently the WiFi is still not working so you are here, you have no phone service to the hospital to being with because the

phone service is kind of crappy in the general building, now you have got no WiFi, you have got nothing else is going on it is just basically bare bones right now.

Terence Russo Wow how much did this cost? Not just the patient risk, because there probably was some patient risk here if you think about it, not having that type of access to information when you have to make quick decisions but even the cost revenue, lost procedures, morale. I mean you probably diverted some patients.

Doctor I mean it got pretty - You would be surprised on how deeply integrated, how deeply dependent we are on technology. I mean here is one when I was listening to this – well I will just turn on and a solution is fixed. It goes deeper than that. When a patient is on an insulin pump for insulin management. That pump could be hacked by that system so no longer could you do that anymore so you couldn't treat patients that had any pumps because of the potentially be an overdose or an under-dose and the liability with that. So everything had to get shut off. And it just goes to show you now 2023 this is happening, as we get more and more dependent on AI stuff and this and that it is just one of these things that is going to wipe everything crazily problematic in the future if such a thing occurs again.

Terence Russo I totally agree with you Doctor. I don't think you can have 100% safety - it is more of a question of when not if a health system gets attacked again – and then with the staff shortages, the cost margins getting tighter and tighter, people are relying on technology to kind of bridge the gap but when everything is integrated, it also means you're gonna have a real catastrophe when the system goes down unless you periodically have some type of backup. It sounds like you relied on some type of Microsoft Teams or instant communication system but that's really kind of life a lifeboat type thing it's not it's not the same functionality.

Doctor Yea, no, so it was extremely inefficient. And that's just to communicate from doctor A to doctor B – from administration A to B – that hey you are not going to be in clinic tomorrow so don't come to clinic or the staff and so forth. But even as we started getting further and stuff started coming aligned, like the dictation system was not functional. So those people that didn't know how to type, they got really slowed down because you had to type all of your notes out. And then past all of that, once it got better, now you have to go back and reconcile all of that stuff. Like what happened, did anyone get hurt? Did we miss anything? Did we miss any patients? You know did we miss a schedule. Like grandpa down the street was supposed to come for his cancer surgery – does he know that he, did someone reach out to him? All of that stuff is still ongoing – it is really mindboggling.

Terence Russo I really appreciate you giving us some of the insights on the ground what it's like because I read a lot of report and papers about how much money it cost, the risk to lives, the reputation. I had a health system where we actually had to close down the ER and divert people 90 minutes away to the nearest hospital for five days And now the county executive is investigating. And eventually this will come out – they start doing autopsies to figure out what went wrong. Why aren't there backup plans or why aren't there replication servers available? But you know, you might have had it - sometimes these hackers they lurk for several months - you don't know how deep this was. It sounds like it was a fairly deep ransomware attack.

Doctor I think so. We also had to go and divert and there was just a lot of things happened and I don't think anyone really knows what the extent was until down the line until the autopsy like you mentioned, and so forth. But as you start to think about this, I had one of my colleagues "oh yea we got hit on the east coast" and "oh yea we got hit and we didn't pay the ransom and we got hit three more times and finally they paid the ransom" - So you know what is going on is – it just seems like, if you take the concept of you never deal with terrorists, you never pay the thing, well then you get stuck in a situation where patients are three weeks without surgery, or this and that. Do you pay? Do you not pay? It is going to continue? What is the solution here? That's going to be the next step – how to prevent these. I don't think it is going to go away any time soon unfortunately.

Terence Russo I don't either no unfortunately. And some of these ransomware attackers, they have reputations and people, I have been told, FBI sometimes says hey pay these guys and they will actually deliver and they will give you your data back. I think it's a bit of a fact and circumstances test. It is generally not a "we never negotiate with ransomware attackers". Because it is so desperate. Last question – how is the morale of the physicians? I would think the physicians probably want to know what the heck happened and how did this happen? This was a major major disruption. I mean this is a month long disruption if you look back on it.

Doctor So, several things. First off, you know as a physician, you always worry about patients – you know what got stolen – what got destroyed and so forth. Delay of patient care is definitely there. There is definitely some patients who were waiting – their family had flown in and so forth to get their cancer surgery and they had to get delayed for a bit so we are just trying to catch that up. That is the first step. What effect on the patients and that is definitely a problem we had to try to figure out. But the second thing was a lot of these physicians, myself included, we get reimbursed by doing surgery and if you don't do surgery you don't get paid. So if you're not operating for two weeks – this is supposed to be the busiest time of the year right? It you're not operating during that time what happens? You know the hospital system is not going to say here we are going to recoup you that. No, so there's that. So the morale goes down. The patient care component, plus all the other stuff, is there legal stuff down the line, you know delay of care, you know this and that, who knows what is going to happen? You know that's the crazy part.

Terence Russo It is a bit of an unknown and there have been some cases now where physicians and hospitals are sued for ransomware because they say it affected the actual outcome of the patient and it has been thrown to medmal. Maybe the hospital system didn't have appropriate data security. Unfortunately I am seeing some of those cases now. It is still new, it's a relatively new, area of law but there will be some consequences here.

Terence Russo I think when you find out more when you get the autopsy - what went wrong? Why did it take so long? What are we doing to avoid this in the future? Those are important questions Doctor that your health system has to ask. And hopefully the physicians will be pushing for that.

Doctor Yea, right now they have been real hush hush and everything in terms of like what happened. But I hope it comes to light exactly what was the source? What happened? Did we fix it and how do we prevent it in the future? It is crazy because we already have to log in every time you see a patient you really have to like re-log and that takes a lot of time and then you start thinking, every several months you have to get a new password – and I ran out of passwords and you don't even know your own password these days – so because there is just a recycling of everything back-and-forth – so maybe there is a new way is it a fingerprint, is it retinal like at the airport you know what is what maybe AI can help in the future to prevent some of these attacks and try to figure stuff out.

Terence Russo Yea, well hey, my condolences. I'm hoping that they get everything under control before you know Christmas. Because I know this is a busy time and thank you so much for sharing what you experienced. This is becoming unfortunately all too common and it's good to hear with you know with the boots on the ground what it's really like. It sounds fairly chaotic. I'm hoping you get sense, Maybe we will even follow up in a couple months, I'd love to know an autopsy to figure out how can we reduce, even if you can't prevent it from happening, how can we prevent it from being so bad? How can we protect the consequences? Two or three weeks of very long downtime for any hospital system.

Doctor Definitely. I do applaud both of you for having this type of conversation so others can at least if it happens to them, or maybe spread the word out a little bit more whoever is listening to the podcast like hey ask that question, what are we doing in case we get hacked? Is there a backup plan? You know just start those questions maybe will spark some progress for someone else in the future for these problems that we had to deal with.

Terence Russo That's right. You know I think so, the conversation. One of the most common questions I always ask my clients, is when was the last time you did a fail over disaster recovery test a full one to see if it will really switch over. You would be surprised people pay for replication services and backup and when they really need it that it doesn't actually work. So it is all too common.

But thank you Doctor so much for your time. This was actually really really interesting and really helpful.

Doctor Well you are welcome. My pleasure.

Philip Hammarberg: Thank you, it was a pleasure speaking with you.