Change Healthcare Cyberattack: Avoid, Safeguard, and Mitigate

By: Philip Hammarberg and Zachary Cohen

Philip Hammarberg: Welcome to the Garfunkel Wild Health Care IT Podcast. My name is Philip Hammerberg, and I'm a senior attorney. And I'm here with Zach Cohen, a Partner with Garfunkel Wild.

Philip Hammarberg: Today we're diving into a pressing issue that has rocked the health care industry, a cyberattack on Change Healthcare, a pivotal player in the pharmacy and healthcare billing industry. Change Healthcare is a software company that is part of United Health Group's Optum Business, which reportedly processes prescriptions for over 67,000 pharmacies, 129 million patients, and handles more than 15 billion health care transactions annually.

Philip Hammarberg: This cyberattack has not only affected military health care services provided by Tricare, but has also led to delays in prescription processing at retail pharmacies nationwide. Change Healthcare has said that more than a hundred of its systems have been affected.

Philip Hammarberg: These solutions include solutions that benefit verification, medical necessity reviews, billing and coding. And it has impacted military, pharmacies, clinical hospitals, and local pharmacies. Zach, what do facilities do about this?

Zach Cohen: Yeah, this is a big problem when there's a cyberattack that's this big that affects so many providers nationwide. The American Health Association has given some advice to all of its facilities, which is first and foremost disconnect from Optum and check your systems for security vulnerabilities.

Zach Cohen: One thing is, you want to make sure that you're not connected to the entity that has an ongoing breach, because the attackers might be able to have vectors to get onto your system if you're still connected.

Zach Cohen: They also advise that facilities should be testing their data backups and checking critical patches are up-to-date for all of their software.

Zach Cohen: This will allow those providers to know that if for some reason they do have to shut down their system, they have all their backups in place, and that if something did get onto their system, all their patches are in order that can help fight any sort of attack that's on their system.

Zach Cohen: They also recommended that each hospital and facility should designate staff to go into shifts for managing the manual processes that are going to have to happen.

Zach Cohen: Phil, as you mentioned, these solutions include solutions that affect benefit verification, medical necessity, review billing and coding. So now, if all these hospitals and facilities can't do those via these solutions with automation, they're going to be doing it by hand, which is going to be very time consuming. It's going to create a lot of questions by their employees of "How do I do this?" So you know, you want to have these staffs in place and shifts that can, you know, help as much as needed.

Philip Hammarberg: And, Zach, I've read that this is suspected to be a nation-state attack. What does that mean to you? And how might a medical provider try to minimize its risk against this sort of attack.

Zach Cohen: Yeah, so a nation-state attack is an attack by what the United States recognizes as an adversary to the national security of the United States, and this includes countries like China, Russia, North Korea, and Iran.

Zach Cohen: What it means to me when I hear that, is that there are certain provisions in a contract that if you don't think ahead of time about the fact that these nation states out there might attack industries that can affect your hospital, your medical practice, you might be putting yourself at risk.

Zach Cohen: So the big thing that comes to my mind is a force majeure provision. Contracts often have provisions that say we're not responsible, the vendors not responsible if there's a problem that happens because of a force majeure, which is like an act of God. That could be a fire, that could be that that could be a flood, it could be an electricity failure. But it can also include acts of war. And it's plausible to take the position that if Iran or Russia or China is attacking a system that that is a cyberattack act of war. And a vendor could take the position that "I'm not responsible now for everything that's now happened and therefore you, customer, are on your own for this".

Zach Cohen: That can be a scary situation for a customer who is, you know losing tons of business or you know, now has to pay third parties lots of money to figure out if their system was affected, because, you know, the vendor system was affected. You want to be able to have someone to go after. The other, kind of connected to this, with the force majeure, a lot of these solutions are cloud based solutions, meaning that they're on the they're on the network of the provider, like Change Healthcare's.

Zach Cohen: These contracts have SLA provisions that often say, "Here's the downtime that we won't be down for more than X amount, and if we are down for more than X

amount, you'll get these types of credits to your monthly fees, or you might even get a termination right". Now, these SLA provisions can also include carve outs or exclusions for force majeure provisions or for emergency maintenance. And you know, it's very safe to say, emergency maintenance can include Change Healthcare taking down its network because there's a cyberattack, and it wants to make sure it doesn't spread anywhere.

Zach Cohen: So all of a sudden, you know, Change Healthcare system could be down for a week, and you might not have any credits coming to you. You might still be having to pay all the fees you were supposed to be paying because of provisions like this.

Zach Cohen: The last thing that comes to my mind is a hospital or a provider's cyber insurance policy. Cyber insurance policies also oftentimes have exclusions for acts of war, which again, if it's a nation-state attack, that insurer is probably going to take the position that it's an act of war.

Zach Cohen: So these are all things that you know, , if a hospital or a provider doesn't think about, their contracts could be at risk where they wouldn't be able to, you know, go after their vendor or go to their insurer to help them with any sort of damages that they get because of this action.

Philip Hammarberg: Those are great points. And at GW, we assist a lot of clients in dealing with contracts related to health care IT. And we're always trying to minimize the risk for our clients.

Zach Cohen: Exactly. We're doing this, for you know, we have a department that does this all the time for hospital systems, large practices, even individual practices. We help all providers with their IT security frameworks and regulatory compliance.

Philip Hammarberg: Unless you have anything else to add, I think we've discussed this event, and I'd just like to thank the listeners for joining us on the Garfunkel Wild Health Care IT Podcast and until next time take care.