GREATER NEW YORK HOSPITAL ASSOCIATION

PRESIDENT, KENNETH E. RASKE • 555 WEST 57TH STREET, NEW YORK, NY 10019 • T (212) 246-7100 • F (212) 262-6350 • WWW.GNYHA.ORG

(SOUNDBITE OF MUSIC)

KATE BASTINELLI, HOST:

Welcome to Perspectives. I’m Kate Bastinelli from the Greater New York Hospital Association and today my colleague Jenna Mandel-Ricci will interview Dr. Mark Jarrett, Senior Vice President and Chief Quality Officer and Associate Chief Medical Officer at Northwell Health. Dr. Jarrett is also a professor of medicine at the Donald and Barbara Zucker School of Medicine at Hofstra University. Let's get started.

JENNA MANDEL-RICCI:

So, Dr. Jarrett, when did you first become involved in cybersecurity at Northwell?

DR. MARK JARRETT:

My involvement started about four to five year ago. It is a result of the merger of my interest in, obviously patient safety and quality, as well as emergency preparedness and the recent fact that I had gotten a master’s in medical informatics.

MANDEL-RICCI:

So the cybersecurity threat landscape has changed quite a bit over the last few years becoming more and more sophisticated. Can you talk a little bit about how Northwell has changed its approach to cybersecurity in order to stay up with these potential threats?

JARRETT:

So Northwell Health attacks cybersecurity in several ways. We've clearly increased our staff. We now have close to 100 people in the Northwell system who actually work on cybersecurity. Recognize that we have 70,000 employees, 23 hospitals, 750 ambulatory sites, so clearly, we are much larger than most people, so we need that type of staff. We also approach it from several levels. The first is clearly what happens with our employees and social fishing because that is really the entry point for many hacking events and ransomware, etc., but in addition, we need to have our firewalls protected, people auditing who's trying to intrude into our system, how it occurs. Finally, Northwell Health doesn't just take an approach on an electronic basis, but we also have to look at physical security. You know, where are a computer closets in the hospitals, are they being protected, can people just access them walking in without a key or are they protected, are they even locked at all? How do people get into the repair areas? These are all things that we have to be aware of, as well as the usual things of trying to get people to keep their passwords up to date.

MANDEL-RICCI:

We know that cybersecurity requires a uniquely multidisciplinary approach. What do you think a person in your role of Chief Quality Officer brings to the conversation of cybersecurity in cybersecurity preparedness?

JARRETT:

I think what a physician brings to the table, or a clinician, is the impact of cybersecurity events. I think that the cybersecurity teams are very well with health care, but they really don't see the downstream effect of what can happen if there is an event, anywhere from losing the ability to use our electronic systems to particular harm to patients because of changes that have occurred in devices, etc. So, we as clinicians really bring that home.

MANDEL-RICCI:

And Dr. Jarrett, following up on that comment. As you bring together all of these different individuals in different roles there often can be a cultural divide, for example between a clinician and someone in IT security or someone in legal are regulatory. How do you all work to continuously overcome those divides and have everyone working in the same direction?

JARRETT:

Well, I'm lucky because at Northwell, which is a truly matrixed organization, we don't believe really a table of organization. We all approach problems in a multidisciplinary way, not only cybersecurity but in many cases we bring the legal team, we bring IT teams together when trying to solve a problem, which may be more clinical then it is even IT. So, people are used to working together. We give everybody a voice and I think that multidisciplinary approach has really been very successful for us and allows us to accomplish more than if it was all directed and coming out of one area.

MANDEL-RICCI:

And Dr. Jarrett, how can external partners, partners like law enforcement agencies, the Food and Drug Administration, and other federal agencies that have a role to play in cybersecurity, how can they assist health care and hospitals in particular have more secure systems?

JARRETT:

The first thing is by providing information, and there is a lot of it out there now. I think it is much better several years ago. There are a lot of alerts that go out that inform hospitals about things that are going on in the nation at other places, so that they can learn what they should be protecting against—they give a lot of advice which is good. I think another important thing though is that, taking a term from health care, that there be a just culture. They have to recognize that if they come in as law enforcement and there's penalties or bad effects because they're reporting things or discussing things that happened at their institution, if they're punished, they’re not going to want to come forward. It really needs to be an open table, much like the airline industry does where people sit down and are free to say anything they can and if they know something went wrong, they can bring it up and there's no retribution for it. It needs to be a just culture, that doesn't mean people aren't held accountable for being negligent, but in most cases it's not a matter of negligence, it's a matter of either resources or just not having the right information, and that's where the regulatory agencies in law enforcement really need to soften their approach somewhat so that things can go on.

MANDEL-RICCI:

I think that point you are making about the role of law enforcement and regulatory agencies and others having, *using* principles of just culture is very important, because this really is a community problem and when you have bad actors that are continuously innovating, we are in a position where we're constantly trying to catch up and the only way we can do that is by sharing and working together.

JARRETT:

As I always remind people in regulatory agencies, you too are patients or your families are patients, so you want us to be able to do this to protect you and your family. This is not a matter of regulatory burden; this should be something that just works well.

MANDEL-RICCI:

And Dr. Jarrett, you are involved with a work group organized by the federal government and charged with future gazing. Can you tell us a little bit about what that group is seeing as emerging cyber threats of greatest concern to health care?

JARRETT:

In that group, we look at the aspect of what new technologies are coming out and what vulnerabilities they present, because the new technologies offer great possibility for improve health care but at the same time, they may cause insecurities in a cyber security system. An example would be machine learning and artificial intelligence. We are all hopefully learning very quickly how to use that to be able to predict patients getting ill quickly, how to prevent diagnostic error—this is a great new evolution in health care. However, it's also apparent that machine learning can be used to break passwords very easily and also the algorithms that are used in machine learning, if they're changed, will alter the results that you get and people who are bad actress may be able to do that. So that's an example of a great new technology that now presents a new vulnerability. Another place is our medical internet of things. There are a billion devices out there from Fitbits to blood pressure monitors that are all wireless, that people are using at home and that's great, it's producing a lot of data which can help us with health care. But the problem with that is they’re often on wireless home systems where people are downloading the information where the username and password are Admin and Admin1, which were the original default ones, which means that somebody can hack into that person's home account and now be able to transmit malware potentially into wherever that is being downloaded in the doctor's office or at the hospital. So, this is another area that we're looking at to say, “yes, this internet of things is going to improve care, but how does this medical internet of things produce problems for us that we have to solve early on in order to prevent health care from being impacted in the wrong way?”

MANDEL-RICCI:

What I hear in that answer is a continuous attempt to balance innovation with security and there's also the issue of layering of systems within health care, so even if you have a new system that is built with security in mind, it might be dependent upon her layered with a system that is 10 or 12 years old that may not have those same security measures in place. Can you talk a little bit about the balance of innovation and security?

JARRETT:

Well, what you’re really speaking about with that is the fact that the ecological environment of IT in most hospitals and health systems is a patchwork of legacy systems. A patchwork that cannot unfortunately be taken away or change very quickly. The cost, both in terms of the financial cost, but also in terms of the actual human capital to do this would be too large, also as health systems come together, they have a patchwork of systems from the hospitals that already had something else and you can't change everything. This makes it difficult because you put new innovations in you not only have to make sure the interact with the things that you know are up to date as you said, but many things that aren't as well up-to-date and it's not as easy as updating your iPhone. We all know that when you update your iPhone you get the alert, you know you hit the button and you install the new software, and of course if you wait till 0.1 it's usually better because if you do it at 0.0, usually there’s a few bugs that now messes up your iPhone. Well, it's the same problem in health care. We need to keep everything up to date, update the software, but that software does not sit to vacuum, it’s not siloed like your iPhone. Therefore, it interacts with all these other systems and when you update one system you must test it first in order to make sure it does not have a bad impact on other systems, especially older legacy systems. And that is why when people go “well how can hospitals not have the latest updates on all their software?” it is a very laborious and time-consuming process that must be carefully done because otherwise truly it could bring down other systems and impact care. So, it's not the simplicity of just updating your iPhone and hitting that install button.

MANDEL-RICCI:

And of course, this is an environment that runs 24 hours a day.

JARRETT:

Yes, it does. You know, I always give that analogy when we talk about patient safety: if the airline industry was like health care, they’d be having to repair 747s that are 70 years old with no spare parts that are flying constantly.

BASTINELLI:

In the next episode, I interview Tom Mustac, Senior Director of Biomedical Cybersecurity at the Mount Sinai Health System. Until then, this has been Perspectives.

(SOUNDBITE OF MUSIC)