Nutter uncommon law

INSIGHTS

"There are many outstanding questions surrounding liability related to data from connected medical devices that courts have yet to settle. While more sophisticated medical devices and the data they collect will save lives, they will also create tempting targets for hackers that will surely generate complex legal issues."

Code Blue: Cybersecurity Vulnerabilities for Medical Device Makers Require Urgent Care

Q: HOW IS THE SHIFT OF MEDICAL DEVICES MOVING TO THE INTERNET OF THINGS AFFECTING THE HEALTH CARE INDUSTRY?

A: Connected medical devices routinely record sensitive health information about a patient. This critical real-time access to information gives these devices an edge over older models. The risk, however, is that this very same connectedness allowing health care professionals to provide more responsive, personalized care also makes the data or the devices vulnerable to hackers.

Q: WHY ARE HACKERS TARGETING THE MEDICAL DEVICE INDUSTRY?

A: There are many reasons. Certain medical records are valuable because it's profitable to monetize health insurance information. Additionally, hospitals and doctors' offices present tempting targets for ransomware attacks because of the urgency of care. In other words, if a shipping company's computer goes down, that is unlikely to immediately cause injury to any person. However, if a hospital's computers go down, the hospital may find it difficult to continue basic health care operations, which could easily (and quickly) lead to life-threatening situations. Thus, a hospital cannot wait a few days—or even a few extra hours—to recover from a ransomware attack, making it very hard to resist paying a ransom, even a large one, to ensure its patients' safety.

Q: COULD YOU SHARE AN EXAMPLE OF HOW MEDICAL DEVICE SPECIALIZATION CAN RESULT IN PATIENT DATA BEING MADE MORE VULNERABLE?

A: One example is orthopaedic surgery; one study estimated that by 2030, 50% of all total knee replacements will be performed robotically with patient-specific data. Robotic-cutting can aid a surgeon with positioning the implanted prosthetic device. Prior to surgery, the manufacturer obtains the patient's medical records and develops a patient-specific program for the robot, so that in effect the patient receives individualized surgery. In the past, manufacturers would not have direct access to patient-specific records and would not be part of pre-operative surgical planning. Under this new regime, however, manufacturers will need patients' X-rays, CT scans, MRIs, and other medical records, meaning that they will now have access to sensitive data about patients that used to be kept entirely by hospitals or doctors.

Q: HOW CAN MEDICAL DEVICE MAKERS GUARD AGAINST CYBER ATTACKS?

A: As with any security plan, the starting point is to build in the concept of security from the outset. Ensure that encryption is in place every step of the way and require multifactor authentication. As companies design their devices they must make them as secure and redundant as possible to protect them from ransomware and other attacks. Companies must implement a policy on how long they will keep patient data, to ensure it is either be disposed immediately or thoroughly anonymized as soon as is possible. Medical device makers also need to be sure that patients are aware of what data the device makers have and how they are using it.

It is also critical for a company to have a written crisis operations plan on how to respond in the event of a cyber attack. Device makers should identify internal and external teams to execute this plan, and must be prepared to rapidly assess what happened in an incident, who is responsible for it, and how the company can handle its legal obligations. Moving rapidly after an incident will minimize the damage.

Seth P. Berman

LEADER
Privacy and Data Security Practice Group
617.439.2338
sberman@nutter.com

David L. Ferrera

LEADER
Product Liability Practice Group
617.439.2247
dferrera@nutter.com

PRESS CONTACT:
Heather Merton
Senior Communications Manager
617.439.2166
hmerton@nutter.com

Code Blue: Cybersecurity Vulnerabilities for Medical Device Makers Require Urgent Care

Q: WHAT DO YOU PREDICT WILL BE CHALLENGING FUTURE LEGAL ISSUES?

A: We foresee a tremendous "battle of the forms" over entities accepting liability in the various contracts that are required between and among doctors, hospitals, device makers, and patients.

Another tricky area concerns the legal concept of the doctor as "learned intermediary" between the patient and the device maker. This defense doctrine states that a medical device manufacturer can fulfill its duty of care to a patient when it provides all of the necessary information to a "learned intermediary" physician who exclusively interacts with the patient. Individualized medicine such as robotic surgery creates a "blurring of the line" between doctor and device maker. Can a device maker continue to rely on this traditional defense?

Finally, hacking incidents may make it difficult to assign liability between the device maker and the doctors. Imagine a scenario where a ransomware attack occurs midway through a surgery, subsequently causing the device to malfunction. Or, a hacker obtains the ability to shut off pacemakers and threatens to do so unless the hospital pays them off. Were these harms foreseeable to the device maker? Would an alternative design have prevented them? Is it the hospital's or the device maker's responsibility to address these problems? These traditional product liability issues can be turned on their head by new technologies.

There are many outstanding questions surrounding liability related to data from connected medical devices that courts have yet to settle. While more sophisticated medical devices and the data they collect will save lives, they will also create tempting targets for hackers that will surely generate complex legal issues.

Seth P. Berman leads Nutter's Privacy and Data Security practice group. Corporations and their boards engage Seth to address the legal, technical, and strategic aspects of data privacy and cybersecurity risk, and to prepare for and respond to data breaches, hacking and other cyber attacks. Seth teaches a Cyber Crime Law class at Harvard Law School.

David L. Ferrera leads Nutter's Product Liability Litigation practice group. Fortune 500 medical device and pharmaceutical companies rely on David's expertise and experience in presenting complex product liability issues to lay juries and courts. David is well-versed in many fields of medical science, including orthopaedics, biomechanics, biomaterials, epidemiology, and pathology.