A New Form of Hacking

Medical technology has come a long way in recent years, with advent of devices meant to improve patient safety and facilitate provision of care by health workers. New types of intravenous pumps deliver fluids and medications with built in safety nets such as hard and soft dosing limits manageable by the hospital pharmacy remotely. New model pacemakers offer monitoring and settings adjustment remotely over the phone, providing increased convenience and flexibility for the patient. Modern insulin and pain pumps with remote programming capability allow changing of dosing parameters.

These are wonderful innovations, but as with most technology the advancements are happening faster than the safeguards for their use can be put into place. It is a growing concern that cybersecurity is insufficient for the susceptibility of these devices to cause harm if they were accessed by an individual with malintent.

New on the scene in recent years are specialists called white-hat ethical hackers who work to expose the vulnerability of medical devices and offer solutions to weaknesses found in the software. Billy Rios and Jonathan Butts are two of the louder voices of this brigade, issuing over 500 advisories to vendors regarding potential weaknesses in their product security. Most companies are cooperative and work toward improving the security of their products – happy for the advance notice and opportunity to avoid a possibly catastrophic problem.

WHAT COULD GO WRONG?

In 2009, researcher Kevin Fu, at the University of Massachusetts, showed the vulnerability of a cardiac defibrillator to hacking which can cause problems such as failure to sense a lethal rhythm and draining the battery making the device non-functional. Jay Radcliffe, an ethical hacker demonstrated ability to take control of an insulin pump and deliver a lethal dose. Billy Rios revealed the vulnerability of Hospira intravenous pumps to hacking and dose alteration done via a hospitals wireless network. The fear is high, valid and led to Vice President Dick Cheney disabling the remote feature on his pacemaker, as a safeguard.

There has been no evidence of direct patient harm related to device hacking to date, but most experts believe it is only a matter of time. Forbes magazine reported an outbreak of "WannaCry" ransomware that affected 48 hospitals in the UK, and several unnamed facilities in the United States. The hackers then demand a ransom for the release of the files threatening to destroy them if their demands were not met. The devices targeted in the U.S. were Bayer Medrad smart injectors which deliver contrast media during imaging studies. The WannaCry caused the injectors to become non-operational for about 24 hours, however, in the UK the ransomware caused complete shutdown of imaging departments.

A lack of industry standard is associated with cybersecurity for medical devices and the concern is that as hospitals update their equipment, they will still not reflect best practices for technology safety.

The FDA has been implementing plans and processes to address this new threat.

GOALS OF MEDICAL DEVICE SAFETY ACTION PLAN:

- Establish a robust medical device patient safety net in the United States.
- Explore regulatory options to streamline and modernize timely implementation of post-market mitigations.
- Spur innovation towards safer medical devices.
- Advance medical device cybersecurity.
- Integrate the Center for Devices and Radiological Health's premarket and post-market offices and activities to advance the use of a Total Product Life Cycle approach to device safety.

AN ARTICLE IN CYBER SECURITY VENTURES OFFERED THESE INTERESTING STATISTICS:

- The United States represents about 40% of the global market for medical devices.
- The average hospital room contains 15-20 medical devices.
- Each medical device has an average of 6.2 vulnerabilities.
- Medical devices used by hospitals have an average use of 20 years per device making them prime hacking targets.
- In 2017, 465,000 pacemakers were recalled by the FDA due to security vulnerabilities with potential to put patient's lives at risk.

PROTECT YOURSELF

Know the product. Investigate and make sure the manufacturer built the device with cybersecurity concerns addressed. Share information via Shared Analysis Organizations which encourages individuals and businesses to identify, detect, and understand vulnerabilities in medical devices. Keep your medical device software up to date; this makes it harder to hack.

Innovations in medical device technology are exciting and provide improvement in patient care and safety and management of medical devices. It is important moving forward to improve the merging of cybersecurity with device development to safeguard patients from the threat of device hacking.

Patty Mitchell, RN, BSN, CLNC is the president of Central Florida Legal Nurse Consultants. Her nursing career has spanned over 24 years, in the hospital acute care setting. She is a graduate of the Medical Legal Consulting Institute and maintains her certification. Patty is the president elect of the Greater Orlando Chapter of the American Association of Legal Nurse Consultants. She has provided consulting services since 2014, to both plaintiff and defense attorneys on a wide variety of cases. She is a member of the National Association of Certified Legal Nurse Consultants, and Sigma Theta Tau, nursing honor society.