CONNECTED MEDICAL DEVICES – FRIEND OR FOE?

The Internet of Things, IoT, now includes medical devices, from those in hospitals to the ones people wear.

But as with so many things, there are pros and cons to this.

The pros for the hospital and medical office devices are that the technicians and doctors get needed information more quickly, almost as soon as the tests are done.

The pros for wearables are also rapid information. Wearable health devices range from reporting-type devices such as fitness trackers, to active devices such as insulin pumps.

Reporting type devices measure and deliver information like number of steps or heart rate. Very helpful in tracking our exercise routines and benefits.

The pros for active devices such as insulin pumps are the real time provision of life saving medication at the right levels for meals and between meals. The pumps are so much easier than the meters, test strips, syringes and insulin supplies needed before.

But there is a dark side. Many IoT devices have minimal to no security making them vulnerable to hackers.

If a hospital medical device is hacked it can provide inaccurate information to the doctor prescribing treatment making it less effective or potentially harmful.

If a reporting type wearable is hacked it is certainly annoying but rarely life threatening.

But, hacking of active devices such as insulin pumps can be fatal if the incorrect amount of insulin is provided.

The challenge is that many IoT devices aimed for a low price point and use technology from third parties. Even if the manufacturer updates it, and some don't, the device manufacturer has to be aware of it and provide it to the end user. The result is many devices do not get updated and security holes remain.

For good security, it must be clear who is responsible. Current thinking from the medical and technical communities is that hospitals and medical practices are responsible for protecting all devices and information on their networks. But the manufacturer is responsible for using secure practices in developing the device. The legal implications are yet to be determined.

The wearables are often controlled by an app on the user's phone making them susceptible to hacks from many directions, the phone itself, wifi and Bluetooth.

In the end, the devices offer much benefit but must be protected. It may come down to caveat emptor, buyer beware, as the buyer or user is the one at risk.

To learn more about cyber protection and education contact Aurora Information Management at info@AIMglb.com or call (888) 773-1920.