Privacy and Security of Health Monitoring Devices

The Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data May 2015 report by the Ponemon Institute revealed that for the first time, criminal attacks were the foremost cause of data breaches in health care (Strauss, 2015). General networks are constantly under attack, but the most common types of directed attacks are on healthcare facilities--from holding databases hostage to targeting individuals such as healthcare workers (Rios, 2015). Cybersecurity needs to be taken seriously as part of the risk management plan.

Minimal compliance (which is encryption/decryption of electronically protected health information) with the Health Insurance Portability and Accountability Act (HIPAA) is not enough to safeguard biometric data and patient records (Baker, Knudsen, and Ahmadi, 2013). The Ponemon Institute reported: 58% of the studied entities had policies/procedures to prevent/detect unauthorized patient data access, loss, or theft; 49% of the studied entities had technology to prevent/detect unauthorized patient data access, loss, or theft; 50% of the entities had performed a 4-factor risk assessment after a security as a required HIPAA procedure (Strauss, 2015).

The problem is that many health management systems (which include devices, networks, software, and hardware) are outdated legacy systems or a mix of new (compliant) technology plus old legacy technology (non-compliant) (Baker et al., 2013). It only takes one device as the weakest link to cause a security gap. Not only is hardware compatibility an issue, software compatibility and robustness is another problem.

Andriole (2014) noted some safeguards to plan for. Physical safeguards include isolation of a suspicious device(s) perhaps even on a separate network with limited personnel access. That way, the higher security network would not be compromised. Other physical safeguards include secure data backup and secure destruction of data (Andriole, 2014). Technical safeguards include firewalls, secure transmission, and secure networks/clouds (Andriole, 2014). Administrative safeguards include security personnel, documentation, and personnel training on established procedures/policies (Andriole, 2014).

Andriole (2014) also noted some tools/concepts for security and privacy. Whether using device, software, or accessing a database, authentication is necessary to verify the identity of the user. Authorization goes hand-in-hand with authentication. Authorization is that component that defines the limitations of the user's access to information (sometimes multiple levels of access for multiple domains of information) (Andriole, 2014). Medical information systems need to be redundant (i.e. have backups) in order to be available to legitimate staff and healthcare workers in order to provide care for patients (Andriole, 2014). Confidentiality measures should also be in place. Portable, removable, mobile, and/or wireless devices/storage increase the risk for protected health information (PHI) vulnerability/loss (Andriole, 2014). USB or other removable memory should be avoided. Data integrity when transmitting data is essential in order to avoid corrupt data or tampered data (Andriole, 2014). Some kind of "handshake" (nonrepudiation) method where the recipient acknowledges the receipt of data is advisable (Andriole, 2014).

Biometric data (e.g. retinal scans, heart beat) to be the new "finger print" or new "social security number" which can specifically identify an individual. When considering implementing any health/fitness technology, security should always be part of the conversation and plan.

References

Andriole, K. P. (2014). Security of electronic medical information and patient privacy: What you need to know. *Journal Of The American College Of Radiology, 11*(12 Pt B), 1212-1216.

Baker, S. D., Knudsen, J., & Ahmadi, D. M. (2013). Security and safety for medical devices and hospitals. *Biomedical Instrumentation & Technology,47*(3), 208-211.

Rios, B. (2015). Cybersecurity expert: Medical devices have 'a long way to go'. *Biomedical Instrumentation & Technology, 49*(3), 197-200.

Strauss, L. J. (2015). Data breach study: Criminal attacks now leading cause. *Journal Of Health Care Compliance*, 61-63.