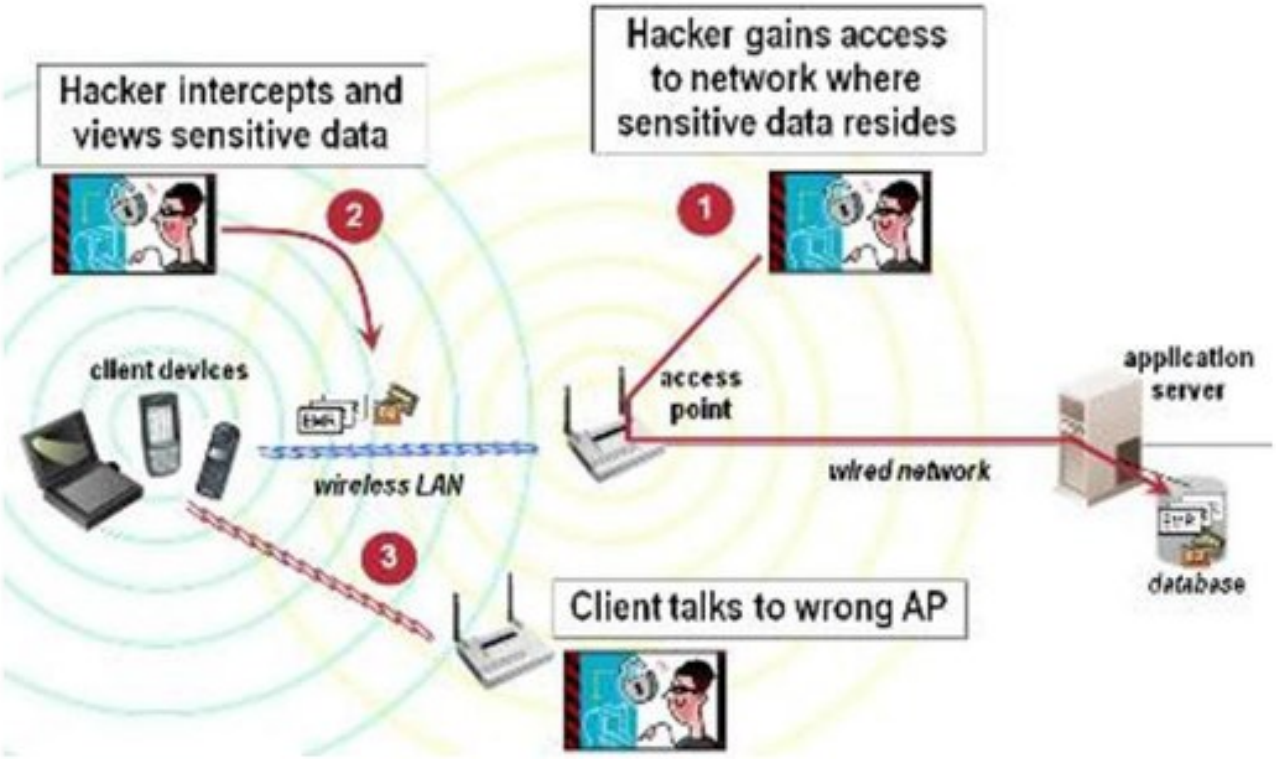
Wi-Fi Security and HIPAA

Laird Technologies

Connecting medical devices to a hospital's Wi-Fi network improves workflow on both the clinical and financial path. With networked devices, a hospital delivers better care to more patients while billing those patients, and their insurance companies, quickly and accurately. Networking medical devices also enables technicians to monitor and manage those devices from a central point of control. Hospitals will not rely on Wi-Fi unless they have confidence that Wi-Fi networks and devices will protect sensitive information that is transmitted over Wi-Fi or stored on networks that can be accessed through Wi-Fi.



Wi-Fi Security Threats

Wi-Fi involves communication between radios that use a specific type of radio frequency (RF) technology to send data to each other over the air. In a hospital, Wi-Fi radios in computing devices (e.g. tablet computers) communicate with Wi-Fi radios in infrastructure devices such as access points (APs) that are connected to the hospital's wired network. The radio waves that travel between the devices can reach waiting rooms and other public areas and even "bleed" through the walls of the hospital to parking lots and other nearby areas. Those RF signals can be viewed by any nearby computing device that is equipped with a commonly available software application called a Wi-Fi sniffer, which makes the contents of Wi-Fi packets viewable. Without proper Wi-Fi security in place, a hacker can use intercepted Wi-Fi packets to do one or more of the following:

- Gain access to the Wi-Fi network.
- View sensitive information that is transmitted over the air.
- Trick users into communicating with the hacker instead of the network.
- To thwart a hacker, a hospital needs to use strong Wi-Fi security. But what type of security is strong enough?

HIPAA and Wi-Fi Security

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the U.S. Department of Health and Human Services Secretary to develop regulations protecting the privacy and security of certain health information. HHS published two documents, the HIPAA Privacy Rule and the HIPAA Security Rule, the latter of which is found in the Code of Federal Regulations (CFR) Title 45, Part 164, Subpart C, entitled “Security Standards for the Protection of Electronic Protected Health Information”. For Wi-Fi client devices and networks, the key part of Subpart C is section 164.312, which lists standards for access control, audit controls, integrity, authentication, and transmission security.

To satisfy the requirements of HIPAA, a hospital Wi-Fi system needs:

- Strong, mutual authentication between every authorized client device and a hospital network where electronic protected health information (ePHI) is housed to ensure that only trusted Wi-Fi clients can gain network access and that trusted Wi-Fi clients are not tricked into connecting to an untrusted network
- Strong encryption of ePHI that is transmitted between a Wi-Fi client and the hospital network
- The Enterprise version of Wi-Fi Protected Access® 2, or WPA2®, satisfies the requirements of HIPAA. WPA2-Enterprise combines:
- IEEE 802.1X for strong, mutual authentication of the Wi-Fi client device and the network
- AES-CCMP for strong encryption of all transmitted data

The combination of 802.1X and AES-CCMP addresses the three security threats discussed earlier. To ensure HIPAA-compliance, a hospital should follow these best practices:

- Ensure that a Wi-Fi client device can gain access to a hospital network only using WPA2-Enterprise with a strong EAP type.
- Configure every trusted Wi-Fi client device to connect only to trusted APs.
- Do not store EAP authentication credentials on client devices.

For more information, watch a replay of the Summit Wi-Fi security webinar [1] or read the Summit white paper [2] on the same topic.

Source URL (retrieved on *05/22/2013 - 8:46am*):

http://www.mdtmag.com/blogs/2012/06/wi-fi-security-and-hipaa?qt-most_popular=0

Links:
[1] http://www.summitdata.com/webinars.html
[2] http://www.summitdata.com/whitepapers.html