

September 2011

Building Secure “Guest Network” WiFi into Healthcare Facilities

by Scott Montgomery (OST)

A growing trend in healthcare technology is to implement “guest” wireless networks within and around the healthcare facility. However, this trend does pose some potential security concerns, if not implemented after considerable planning. This article provides some pointers, but cannot be considered a comprehensive guide to securing wireless technologies.

The primary concern in the creation of a guest wireless network should be isolation. Isolation of the wifi network from all production networks, and isolation from the production internet connection are both critical. Our experience has shown that this is often overlooked in an effort to establish a guest network quickly and economically.

Without isolation, a visitor using the guest network may have the ability to establish connectivity to critical systems, or eavesdrop on communications. This is obviously of great concern within healthcare.

Planning for a separate internet connection is also necessary. Because the internet connection is often an important communication link in healthcare, sharing this connection with visitors is not a good idea. Visitors may use a considerable amount of bandwidth as they watch videos, surf the web and play online games. This additional bandwidth usage may have adverse effects your production environment. But bandwidth is only one concern. A visitor may also perform unauthorized internet activity that could result in a major security concern for the organization. Because you don’t have control over what the visitor is doing, you don’t want to take the responsibility for this person’s activities.

The guest network should be named so that the SSID is clearly named for guest and visitor identification. For example, use a name like “ABCHEALTHVISITOR-WIFI” or “ABCHEALTHGUEST”. Clearly naming your network will reduce confusion.

Requiring that a visitor acknowledge a usage policy for your guest wireless network is also a good idea. Use this policy to communicate what you intend to have this guest network used for. A policy web page can be displayed in the visitor’s internet browser prior to being provided access to the internet.

The organization should also consider limiting or restricting bandwidth speeds. Guest networks are often used to download copyrighted materials such as music and movies. Not only are these files large, their downloading/uploading is often tracked by the copyrighted owner. If your guest network is used regularly for distributing copyrighted materials, you may find that your Internet Service Provider will disconnect you.

Implementing Port Isolation is also highly recommended. This process restricts one wireless device communicating with another wireless device. The practice is recommended because it reduces the ability to spread worms and viruses.

Your guest network should also not be used by other health care providers such as visiting physicians. Because a guest network is normally not encrypted, a physician's use of the network could result in a HIPAA breach by exposing ePHI to other user of the guest network.

To summarize, a guest wifi network should consider the following:

- Clearly name the guest wifi network for quick recognition by visitors and guests.
- Isolate the guest network from your organization's private internet connection and all other production networks.
- Implement a Privacy and Policy Statement Web Page that requires the visitor or guest to acknowledge the statement prior to gaining access to the internet.
- Communicate via the Policy Statement that the guest network is for the private use of the organization's visitors and guests that that the organization takes no responsibility for its use.
- Communicate via the Policy Statement that the guest network is not intended to be used by a healthcare provider for business use.
- Implement Port Isolation to reduce the spread of worms, viruses and eavesdropping.

As always, verify that this network is included in your annual Information Technology Security Assessment process. Regularly testing the network for vulnerabilities and security weaknesses is necessary to assure your organization is exceeding HIPAA Security Standards.

Scott Montgomery joined OST in the spring of 2009 as the Manager of the OST Security Practice. Scott comes to OST with over 25 years of IT and IT Security related experience.