



The Do's and Don'ts of Deploying Networking for Healthcare Facilities

As healthcare facilities increasingly turn to the latest life-saving technologies to ensure their number one objective—**treating and protecting patients**—it's become increasingly important for those same facilities to ensure **24/7 network connectivity**.

While a robust wireless infrastructure plays a critical role in ensuring life-saving technologies, it's also now being called upon to meet the rising demand for data from medical staff, patients, and visitors, all the while ensuring the physical well-being of more vulnerable patients.

Helpful DO's and DON'Ts When Installing Wireless Access Points in Healthcare Facilities

By their very nature, wireless access points (APs) are installed on ceilings, high on walls, or other open locations to help provide the best possible wireless coverage. And while it's important for a wireless designer to consider how the AP will be blended into the environment without compromising performance, it's equally important to place emphasis on meeting important physical requirements for infectious disease control measures that help ensure the physical well-being of more vulnerable patients and regulatory compliance.



Some helpful DO's and DON'Ts:



DON'T: Poke holes through ceiling tiles to pass antennas or cables; this is NOT acceptable in hospitals, as these openings in the ceiling readily pass dust and fungal spores.



DON'T: Lift ceiling tiles to service above ceiling access points; this is restricted due to the Infection Control Risk Assessment Procedures (ICRA).



DO: Mount in a wireless access point (AP) enclosure that permits access to the equipment and connection to the data cable without lifting or penetrating the suspended ceiling.



DO: Ensure that you comply with the Healthcare Information Privacy and Portability Act (HIPAA) Paragraph 64.310 Physical Safeguards which states, "A covered entity must, in accordance with 164.306 (a)(1) Standard: Facility access controls, implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed while ensuring that properly authorized access is allowed."



DO: Remember that many ceilings act as fire and smoke barriers, and penetrations in such ceilings are restricted.

Aim for Protection, Convenience and Performance

It is possible to ensure protection and security of wireless equipment without compromising connectivity or performance of the network. How? Look for wireless AP enclosures that can provide some, if not all, of the following:

- Ability to replace a standard 2' x 2' suspended ceiling tile.
- Ability to made lockable, ensuring the wireless infrastructure and associated cabling is secure.
- Some models conceal the AP, antenna and cabling behind a plastic dome. Other models recess the AP flush to the ceiling, revealing only the "antenna face" of the access point.
- It includes a metal back-box for fire-rated ceilings, which permits easy access to the AP and cabling without having to open the plenum space, facilitating future technology upgrades.
- It simplifies ICRA procedures while simultaneously providing optimal wireless coverage, saving time and reducing costs over the long term.

Ultimately, the ability to ensure patient safety while maintaining reliable network connectivity remains the goal and it's an installer's job to find the right Wi-Fi AP enclosure and mounting solutions for unique healthcare environments and venues.

Remember that no matter what vendor is selected, make sure they can help your wireless designers to address all the necessary standards, code compliances and ICRA procedure simplifications necessary, while also maintaining the performance and aesthetic challenges present in hospitals.

oberonwireless.com

sales@oberonwireless.com

877-867-2312