INDIO NETWORKS

Connected Healthcare

Helping healthcare leverage WiFi for bettering the lives of healthcare workers and patients.

Introduction

The world around us is already extensively connected. The presence of WiFi is dominant and exists across almost all verticals. Healthcare has not been an exception. Healthcare facilities today are getting connected at a rate much faster than ever before. WiFi in healthcare facilities has been known to be an additional support to patients in aiding their recovery by keeping them constantly connected with their loved ones.

The number of connected healthcare devices & healthcare IoT is growing at a fast pace. These IoT enabled devices need medium of communication through which they transmit real-time data on to the monitoring systems. Many of these devices are WiFi enabled or need WiFi network to operate. WiFi is fast, easy and reliable for communicating data securely with minimal cost.

Guest WiFi is touted to be one of the major requirements in the healthcare space. Visitors and Patients in hospitals expect to receive good WiFi connectivity during their visit or stay in the premises. Hospitals often need to separate the access of patients from visitors and offer differentiated services.

WiFi enabled asset tracking is another important functionality of WiFi use in health care. Healthcare facilities have extremely expensive machinery in use. This machinery can be tracked using low-power BLE and WiFi. Hospitals can offer free WiFi to the patients and their kin, helping them engage with their loved ones, keeping them connected at all times can greatly help their psyche and allow them to heal better, and faster. Secure WiFi networks and encrypted data allow us to achieve this objective.

The healthcare data analytics market will reportedly rise to $50B by 2024 [1]. Data analytics will help doctors and hospitals offer personalized services to their patients and optimize the use of resources.

(C) 2021 INDIO NETWORKS LLC. ALL RIGHTS RESERVED

Key Requirements for Healthcare WiFi

- Fast, Reliable and Affordable WiFi to visitors and patients
- High Availability
- Strong Security Posture to protect user privacy and sensitive data
- Single Console Management
- Integration with Patient Management Information Systems
- Different class of service (patients, visitors, staff, etc.)
- Low infrastructure cost
- Optimized for healthcare IoT

In Depth on WiFi services for Healthcare

Let us take a detailed look at what healthcare services really require from WiFi.

Securing Critical Patient Data

Healthcare & patient data is one of the most sensitive categories of data out there. Healthcare records are protected by law and leaking healthcare data to anyone is a crime that attracts harsh punishment. How can healthcare facilities secure their data? By securing their network. A lot of hospital data is routed through WiFi, having in place robust mechanisms to identify and eliminate potential threats are important. The WiFi itself should be very secure to prevent unauthorized access into the network. Healthcare in the past has suffered heavy costs due to breaches.

According to reports, a single data hack can cost the industry up to $2.2M, with its cumulative value going upwards of $6.2B [2]. When it comes to healthcare, we cannot stress enough about how necessary it is to secure your networks.

(C) 2021 INDIO NETWORKS LLC. ALL RIGHTS RESERVED

Partitioning Patient, Staff and Guest WiFi

Patient, Staff and Guest networks must be segregated inside healthcare facilities. Staff members might use wireless network to transmit sensitive patient data between devices and people. Securing this data is of utmost importance. Similarly, patients and guest need separate data networks. Hospitals might offer Internet connectivity free to patients but charge the guests. WiFi networks should be flexible to offer different layer of access to different stakeholders.

Bandwidth Management

Bandwidth is always a scarce resource and healthcare sector is no exception. Connected hospitals move vast amounts of data every minute, if bandwidth is not metered properly across all devices & machinery, it can create bottlenecks resulting in inadequate bandwidth to all devices. Mission critical machinery that transmits sensitive data must be given a higher priority and a greater rate of bandwidth should be assigned for the hotel staff and doctors. Devices connected to guest WiFi should be provided different class of service compared to the other devices.

Policy Management Function

Healthcare WiFi should not be used for committing illegal acts. The hospital can be held liable for illegal activities conducted through its network. The best way to protect against it, is to enforce strict access policies, filter illegal content and track user activities on the network. It is important for the wireless networks to be protected from hacking attacks, rogue devices, DoS attack and similar activities to ensure safe and secure connectivity to the users.

(C) 2021 INDIO NETWORKS LLC. ALL RIGHTS RESERVED

Web Logging and URL filtering

Web logging is necessary to store records of what websites the user has accessed in their connected time. Several countries have regulations to track user activities and web browsing history on the networks. Sensitive URLs should be blocked through URL filtering. URLs banned by the regulatory authorities should not be available for access.

WiFi coverage

Providing ubiquitous Internet access across the hospital premises is important. System integrators need to conduct wireless survey to ensure all the area is covered with WiFi signal. They also need to plan the capacity of the network based on the user concurrency.

Deployment Challenges

Hospitals are information sensitive places. The primary concern of a healthcare network is ensuring its complete security. However, with that said, there are a few other things that need to be checked in a healthcare facility like:

- Network planning
- RF Design
- Ensuring maximum WiFi coverage
- Securing the users
- Segmentation of users

(C) 2021 INDIO NETWORKS LLC. ALL RIGHTS RESERVED

How we help Healthcare with WiFi.

Indio offers a single vendor, end-to-end Healthcare WiFi solution with an emphasis on a strong security posture & a tough firewall to protect critical patient data. We offer complete range of WiFi access points, controllers and cloud solutions that can be deployed to build a robust and secure wireless network. IT administrators can easily manage and monitor the entire network setup from a single console. Separate network access policies can be setup for different stakeholders to ensure the available Internet bandwidth is fairly used. The same network can be utilized to deploy an asset tracking solution using BLE tags to ensure expensive medical equipment is tracked in real-time.

Some of the important features for healthcare WiFi are as follows:

- Single Console Management
- Integration with Directories services like LDAP / AP / G-suite
- Network Discovery & DHCP IP Assignment
- Dynamic VLAN management
- Integration with Patient Management Information System
- User Authentication
- Policy Enforcement
- Bandwidth Flow Control
- Access Point Management
- Live coverage of AP & heat maps
- Real-Time traffic information

(C) 2021 INDIO NETWORKS LLC. ALL RIGHTS RESERVED

Implementation

Indio provides a complete wireless networking solution for hospitals, doctor clinics and other medical facilities. Our system consists of UniBox network controller, indoor and outdoor UniMax access points and range of managed switches. UniBox controller is placed between the ISP and the Access Points. L3 switches connect the ISP to the UniBox, and L2 switches connect the Access Points to the UniBox. The UniBox essentially functions as an intermediary between the end-users and the internet. UniBox can configure policies based on bandwidth, policy and routing that are to be applied to end-users.

Since network security is the primary concern of healthcare facilities. UniBox comes with a range of features to secure the network and internal users. You can set up multiple VLANs to segregate traffic for in- patient WiFi, out-patient WiFi and Staff WiFi. UniBox and WiOS offer 802.1x /WPA2 Enterprise security for staff users and seamlessly integrate with LDAP or AD systems.
Staff SSIDs are separated from other SSIDs, and offered higher protection, a more robust security protocol 801.x, or WPA2E, for authentication. Out Patient VLANs are also separated as per local regulations to protect the data present in all levels of the healthcare facility.

UniBox and UniMax Access Points come in different models to support different use-cases.

UniBox, when deployed with UniMax APs work as a network monitoring system from where you can control and configure all UniMax APs in the network through a single dashboard. With Zero Touch Provisioning, you can get the entire network of Access Points up and running in less than 20 minutes. All UniMax Access Points can be auto-configured through UniBox.

(C) 2021 INDIO NETWORKS LLC. ALL RIGHTS RESERVED

UniBox comes with a loading balancing mechanism that utilizes all available bandwidth effectively by aggregating bandwidth from multiple ISPs. If in case the primary connection fails, then UniBox smoothly transitions on to the secondary or standby connection with a responsive failover mechanism. This ensures that downtimes are kept as low as possible at all times, this is especially important in a healthcare facility where medical equipment constantly broadcast data to doctors and other staff working in the facility.

Although we recommend using UniMax access points for optimum experience, Indio's UniBox controller solution is vendor-agnostic and works with access points from any vendor.

Solution Benefits

We have served over thousands of patients in healthcare facilities in several countries across the world. Patients have reported an enjoyable WiFi experience facilitated by our solutions. Here are a few ways in which our solutions impacted WiFi in healthcare:

- Patients reported a comforting experience by connecting with their loved ones through seamless WiFi
- Hospitals deployed fast and reliable staff access
- Seamless Internet experience from any place in the premise
- Managing in-patient, out-patient and staff WiFi made easier
- Ensured critical medical systems had secure and reliable connectivity
- Solution very cost effective when compared to our competitors
- Easy integration of third-party APs
- Simple guest on-boarding

(C) 2021 INDIO NETWORKS LLC. ALL RIGHTS RESERVED

- Fast and Cost-Effective Deployments

Connect with our sales team and help improve quality of life with wireless.

sales@indionetworks.com

US: +1 (888) 280 4112

IN: +91 (20) 6715 7379

(C) 2021 INDIO NETWORKS LLC. ALL RIGHTS RESERVED