MyConnectSolutions

HIT BEST PRACTICES FOR FEDERALLY QUALIFIED HEALTH CENTERS

TABLE OF CONTENTS

INTRODUCTION

In the constantly evolving world of healthcare IT (HIT), it's hard to stay up-to-date with the latest tools and technology. This is especially true for Federally Qualified Health Centers (FQHCs), where limited staff and resources can make implementing widespread changes even more challenging.

As a result, FQHCs commonly encounter a number of HIT-related challenges, including:

- Slow, unreliable EHR systems
- Old phone systems and unmanaged call centers
- Lack of IT security and backup solutions
- Difficulty managing and integrating multiple vendors
- Exposure to data loss or patient data breaches

While facing these challenges and more, FQHCs are also under pressure to improve the patient experience, implement more digital and telehealth services, and improve access to electronic patient health data. With so many factors at play, identifying and implementing the best HIT solutions can become a daunting task.

At MyConnectSolutions, we specialize in offering HIT solutions tailored specifically to FQHCs. As a result, our team has become deeply familiar both with the unique technology needs of FQHCs – and the best, most cost-effective solutions that exist in the market today.

In this white paper, we'll identify eight of the most important HIT best practices that every FQHC should adopt – and compare them with the most common legacy solutions currently in use. We hope you can use this information to not only evaluate the current strength of your own IT systems – but to implement new and better solutions that offer a higher level of service to both patients and providers.

8 HIT BEST PRACTICES FOR FQHCS

01 NETWORK INFRASTRUCTURE

Common Solution: **IPsec VPN**
Industry Best Practice: **SD-WAN**

Just a decade ago, a virtual private network (VPN) represented the gold standard of network infrastructure. By connecting a series of firewalls together, VPNs have historically enabled Federally Qualified Health Centers (FQHCs) to maintain network security through end-to-end data encryption. However, the increase in data, software, and Voice over Internet Protocol (VoIP) usage, combined with advancements in cloud-based networking technology, make VPNs a poor choice for today's FQHC.

The biggest drawback to VPNs are issues related to network speed and performance. For FQHCs with multiple locations and large networks, this can result in serious latency issues that interrupt voice and video transmissions.

To avoid these quality of service issues, we recommend that FQHCs transition to a software-defined wide-area network, or SD-WAN. Using this type of network, FQHCs can simplify networking operations while ensuring high availability and predictable service for their most critical applications.

For example, by using an SD-WAN, FQHCs can prioritize network performance based on traffic type – meaning your most important traffic (like VoIP or EHR systems) will always be up and running. In addition to these advantages, an SD-WAN offers simplified cloud-based management, enhanced security, flexibility, and reliability.

02 NETWORK CONTINUITY

Common Solution: No network continuity
Industry Best Practice: SD-WAN and fixed wireless

Like any healthcare organization, FQHCs depend on a stable network connection to serve patients on a daily basis. When a circuit fails, patient care is interrupted. And in our experience, most FQHCs do not have a backup solution in place that allows for seamless network continuity in the event of an outage.

The industry best practice for network continuity is a combination of an SD-WAN and a fixed 5G wireless connection. By combining these two powerful technologies, a network can automatically switch over to wireless network service when a connectivity issue is detected.

The best part about this backup network is that it connects automatically. There’s no need to reconfigure your existing network or manually change the gateway. With an SD-WAN, when one gateway fails, it automatically transfers traffic to a new connection.

This fast, automatic connection means you’ll never be without a network connection.

03 DATA BACKUP

Common Solution: Tape or onsite backup
Industry Best Practice: Cloud backup

When it comes to home entertainment, we all abandoned VHS tapes a long time ago. But across many FQHCs, a facility's most important data is still being physically stored on magnetic tape backup drives or onsite servers.

Obviously, any type of physical data backup comes with limitations. Not only do you need to physically protect the storage device itself, but restoring data from tape drives can be a frustrating and time-consuming process.

For that reason, we recommend FQHCs transition away from physical tape or onsite server backups to a cloud-based storage solution.

With a cloud data backup, all of your most important information is automatically backed up into the cloud. You never have to worry about storing, updating, and protecting local data. And if you ever need to restore data, it can be accomplished in a matter of minutes.

04 DISASTER RECOVERY AND BUSINESS CONTINUITY

Common Solution: No disaster recovery plan

Industry Best Practice: Cloud-based backup and recovery

Today, most FQHCs still rely on onsite servers for data storage. And without a reliable disaster recovery plan in place, a server crash can be catastrophic.

In healthcare, just a few hours of downtime can have huge implications. But if a damaged server needs to be replaced, that restoration time can take up to a week. That’s why we recommend FQHCs adopt a cloud-based backup and recovery system.

When replacing a physical server, an FQHC can waste days waiting for equipment to be delivered and installed. But with cloud-based backups, your system can be up and running in a few hours.

Best of all, a cloud-based backup solution mirrors a live production of your system in the cloud. This continuous backup means users can even restore their in-progress work – ensuring no data is lost in the process.

05 VOICE OVER INTERNET PROTOCOL (VOIP)

Common Solution: Third-party VoIP service
Industry Best Practice: Network-based VoIP service

There is no shortage of third-party VoIP providers serving the healthcare market. And while each provider offers its own unique combination of features and pricing, they can all cause quality issues when running on a large FQHC network.

Voice issues can create significant problems for FQHCs. And correcting these quality concerns can be frustrating. In many instances, it's common for the network provider to blame the VoIP company – while the VoIP company says quality issues are related to the speed of the network. Not only does this constant blame shifting make it hard to pinpoint the source of a problem, but it also delays the search for a practical solution.

To avoid these issues, we recommend using VoIP services that are offered by your network provider. By using the same vendor for voice and internet, FQHCs are able to guarantee class of service for voice data. That means your voice data will always be prioritized on the network – resulting in clear, reliable calls.

06 CIRCUITS

Common Solution: **Coax cable**
Industry Best Practice: **Fiber-optic cable**

In most FQHCs, copper-based coaxial cable is the circuit material of choice. While coax is inexpensive to run, it also results in reduced bandwidth and inconsistent network speeds.

Replacing coax with fiber-optic cable helps improve network performance, thanks to faster, dedicated network speeds and low-latency. As a result, networks with fiber-optic circuits will experience higher network reliability and better voice quality. This makes it ideal for use in FQHC networks.

In addition to these performance benefits, fiber-optic cable is a much more secure option, compared to coax cable – which is an added benefit for HIPAA-compliant networks.

07 FIREWALL

Common Solution: **In-house managed firewall**
Industry Best Practice: **Third-party managed firewall**

Firewalls are essential to network security in FQHCs. By monitoring incoming and outgoing network traffic, these devices are key to blocking potential security threats and establishing secure, controlled internal networks.

While many FQHCs choose to use an in-house firewall that's self-managed by their own IT team, the industry best practice is to use a third-party firewall that's managed by your network provider.

Security threats are constantly evolving – and hackers become more sophisticated with each new attack. For this reason, self-managed firewalls can leave networks more vulnerable to a data breach. Third-party firewalls, on the other hand, have a dedicated team that's focused on continually detecting suspicious activity and addressing network security risks.

Not only do third-party firewalls offer stronger, more robust protection. But they also protect FQHCs against organizational liability in the event of a data breach. When using a self-managed firewall, your organization can be liable in the event of an attack. But if your FQHC uses a third-party firewall, damages incurred by your organization will be covered by the network provider's insurance.

08 SWITCHES

Common Solution: **Old, unmanaged switches**
Industry Best Practice: **Managed Cisco Meraki switches**

The job of a network switch is simple: To send data to individual devices within your network. But depending on the age of your network infrastructure, the existing switches may be slowing down your network considerably.

Upgrading to modern switches, like those made by Cisco Meraki, can result in significantly faster speeds. And when they're managed by a network provider, you can reduce the need for in-house IT support when a switch goes down.

Instead of asking your IT team to find a physical solution to a switch issue, managed switches leave the work to the carrier – who will send a technician to address any problems.

ADOPTING HIT BEST PRACTICES

After reviewing these Health IT (HIT) best practices for Federally Qualified Health Centers (FQHCs), you may be wondering: **How can I upgrade my network to align with the current best-in-class standards?**

If you're looking to adopt any – or all – of these HIT best practices, you generally have two options: Identifying and implementing your own individual solutions, or working with a managed services provider like MyConnect Solutions.

Advantages of Using a Managed Services Provider

The truth is, most Federally Qualified Health Centers lack the staff and resources needed to stay up to date in the constantly evolving world of healthcare IT. That's why we created our MedConnect Platform: to help FQHCs implement and manage best-in-class HIT solutions at a fraction of the cost.

MedConnect combines the best, most affordable HIT services into a single integrated platform. Our full range of solutions are designed to meet the complex needs of FQHCs, and every service is backed by 24/7 expert support. As an FQHC, MedConnect can help you:

Improve Access. Transform your patient experience with always-available, digital access to appointment scheduling, tests and EHR data.

Save Time. Leverage the latest tools to improve the efficiency of staff and providers.

Reduce Costs. MedConnect's managed services approach gives you access to state-of-the-art technology, reducing the in-house resources needed for IT support.

Improve Access. Transform your patient experience with always-available, digital access to appointment scheduling, tests and EHR data.

Eliminate Outages. When networks are down, patient care stops. Our IT infrastructure services enhance the reliability of your network to help keep you up and running – no matter what.

Get 24/7 Support. MedConnects dedicated support team is always on call.

To learn how we can help your organization implement the best practices outlined in this white paper, we recommend **scheduling a free 30-minute consultation** for a HIT gap analysis.

CONDUCT YOUR HIT GAP ANALYSIS

At MyConnectSolutions, we've helped Federally Qualified Health Centers just like yours implement HIT best practices – while saving millions of dollars by reducing their annual IT expenses. Sound too good to be true? Let us calculate your savings using your actual IT expenses and a customized **MedConnect** quote.

To conduct a customized HIT gap analysis, we follow this simple process:

Step One: Discovery

To learn more about the unique needs of your FQHC, we'll start by scheduling a free 30-minute consultation. During this meeting, a member of our team will learn more about your current HIT systems and identify areas for improvement.

Step Two: Gap Analysis

After our initial discovery meeting, we'll use the information we gathered to produce a gap analysis of the IT, infrastructure, and telecommunications systems used at your FQHC. This analysis will help you compare your current IT platform to industry best practices.

Step Three: Customized Quote

Following the gap analysis, we'll provide a custom quote that outlines the cost of switching your current IT services to our MedConnect platform. Using your current IT costs, we can calculate your projected savings – providing an accurate analysis of your return on investment.

Schedule Your Discover Session Today

Ready to learn how you can quickly and easily implement HIT best practices with MedConnect? Schedule your free 30-minute consultation by emailing **ali.rida@myconnectsolutions.com** or visiting **myconnectsolutions.com.**

HIT Infrastructure	Best Practice
Network Infrastructure	SD-WAN
Network Continuity	SD-WAN and fixed wireless
Data Backup	Cloud backup
Disaster Recovery and Business Continuity	Cloud-based backup and recovery
Voice over Internet Protocol (VoIP)	Network-based VoIP service
Circuits	Fiber-optic cable
Firewall	Third-party managed firewall
Switches	Managed Cisco Meraki switches