HEALTHCARE MANAGED IT SERVICES CASE STUDY

# When your IT vendor doesn't understand healthcare, the gaps show up everywhere. Here's how USOC fixed it.

A 35-provider urology practice across 8 Carolinas locations replaced years of reactive, undocumented IT with a fully inventoried, secure infrastructure. The first 30 days told the whole story.

Urology Specialists of the Carolinas (USOC) is one of the region's largest urology practices, with 35-plus providers seeing patients across 8 locations. As the organization grew, its IT environment didn't keep pace. Legacy systems ran without documentation. Security protocols had never been established. And a series of MSP relationships had left behind a patchwork of partial fixes, unresolved vulnerabilities, and no clear picture of what was actually running in the environment.

When Stephanie Santos joined as Operations Services Coordinator, she became the first point of contact for every IT issue across the organization. She stepped into a situation where nothing had been inventoried, nothing had been cleaned up, and the team had no reliable way to know what was at risk. The previous vendor had been reactive at best, patching problems as they surfaced rather than building anything that held.

> **There weren't any proactive solutions with our previous MSP. When we would have issues, it was a lot of band-aids. We needed someone who knew what the healthcare field entailed and benefited us.**

**STEPHANIE SANTOS**

Operations Services Coordinator | USOC

**Organization:** Urology Specialists of the Carolinas (USOC)

**Specialty:** Urology

**Size:** 35+ providers, 8 locations

**Location:** Carolinas

**EHR/PM System:** ModMed

**Focus Service:** Managed IT / Infrastructure Assessment / Security

**Challenge:** Undocumented infrastructure, reactive-only MSP support, no healthcare IT expertise, zero ModMed knowledge

**Result:** Full asset inventory in 30 days, security gaps remediated, reduced downtime, reliable ticket resolution

# The challenge

## What it looks like when healthcare IT has been neglected for years

The problems at USOC weren't the result of one bad decision. They had built up over time, layer by layer, as each MSP relationship failed to deliver and left the next one with less documentation and more debt to work through.

Stephanie inherited all of it at once. No asset inventory. No security framework. A ticket system that generated records but didn't ensure resolution. And a team of providers depending on ModMed every day with an IT vendor who had never worked in it.

### What had to be solved

- **No documentation, no visibility.** The IT environment across 8 locations had never been properly inventoried. Nobody knew with confidence how many devices were on the network, how many user accounts existed, or how old the equipment actually was.
- **Reactive support with no follow-through.** When issues arose, the previous MSP responded. But responses weren't resolutions. Tickets sat open. Follow-up was inconsistent. Stephanie spent significant time tracking status on problems that should have been closed.
- **No expertise in healthcare IT or ModMed.** USOC runs on ModMed. Their previous vendor had no experience with it, which meant they couldn't anticipate the clinical workflow implications of IT decisions, and they couldn't support the system the providers depended on most.
- **Security gaps nobody had quantified.** Without an inventory and without healthcare-specific security knowledge, vulnerabilities had accumulated without anyone knowing their scope. Legacy accounts were active. Unknown devices were on the network. The exposure was real but unmeasured.
- **Manual troubleshooting across 8 sites.** Without centralized device management, every location required separate, manual effort. Problems at one site didn't inform how others were managed. The operation scaled in patients but not in IT structure.

> **They assessed how many devices we had. They looked at our servers, how many users, how many devices, how many servers, and the age of our equipment.**

**STEPHANIE SANTOS**

Operations Services Coordinator | USOC

# How we approached it

## Start with an honest picture. Then fix what matters most.

Focus came in and did something the previous vendors hadn't: they looked at everything. Before offering recommendations or making changes, the team conducted a full infrastructure assessment across all 8 locations. Every endpoint, every server, every user account was accounted for. Stephanie got the first complete picture of USOC's IT environment that the organization had ever had.

From there, the work moved in a deliberate order. The most urgent security issues came first. Legacy access was removed. Unknown accounts were cleaned up. Device control was centralized so the team could manage the full environment from one place rather than bouncing between locations. Security gaps were ranked and addressed in priority order rather than left as a list.

What changed alongside the technical work was the communication model. Tickets had notes. Follow-ups were consistent. Stephanie didn't have to chase status on open issues because the team was proactively updating her. For a coordinator who had spent months being the one person tracking everything manually, that shift was significant.

### From there, we followed a clear path

- **Full infrastructure assessment across all 8 locations** Every endpoint and server was scanned and documented, giving USOC a complete, accurate inventory of its environment for the first time.
- **Legacy access removal and account cleanup.** Unknown and inactive accounts were identified and removed. The attack surface that had been quietly growing for years was reduced in the first month.
- **Centralized device management.** Device control was consolidated, so the team could monitor and manage endpoints across all locations from a single system rather than handling each site manually.
- **Security gap remediation, prioritized.** Vulnerabilities were catalogued and ranked. The highest-risk issues were addressed first, giving USOC a clear roadmap rather than an overwhelming list.
- **Reliable ticket resolution with real communication.** Every ticket came with notes, updates, and consistent follow-up. Stephanie could see progress without having to ask for it.

> **I can't say anything better about them. Focus put us at ease, kept giving us resources, and they were a great choice for us.**

**STEPHANIE SANTOS**

Operations Services Coordinator | USOC

# What we built together

## Thirty days in, USOC knew more about their environment than they ever had.

The first 30 days set the tone for everything that followed. By the time the initial assessment was complete, USOC had a full inventory of every device, server, and user account in their organization. Legacy access was gone. Device control was centralized. Security gaps had been identified, ranked, and the highest-priority issues were already being addressed. But the operational shift mattered just as much as the technical one. Stephanie was no longer the person holding the whole IT picture together by herself. Tickets were resolved and closed. Follow-ups happened without her prompting them. The practice had a vendor who understood what healthcare IT actually required, and it showed in how they worked.

| Metric | Result |
|---|---|
| Time to full asset inventory | First 30 days |
| Endpoints and servers scanned | All — across 8 locations |
| Legacy and unknown accounts removed | Completed in initial assessment |
| Device control | Centralized |
| Security gaps | Identified and prioritized for remediation |
| Downtime across clinical locations | Reduced |
| Ticket resolution | Consistent follow-up and closure |

## Not sure what's actually running in your infrastructure?

**Find out before something else does.** Most healthcare practices have more exposure than they realize. Undocumented devices, inactive accounts, aging equipment, and security gaps that never got prioritized because the previous vendor never looked that hard. An infrastructure assessment is the fastest way to know where you actually stand.

Focus works exclusively in healthcare. We know ModMed, we know what regulatory exposure looks like in a multi-site practice, and we know how to communicate what we find in a way that makes sense to the people running the organization. If you want to know what's hiding in your network, let's start there.