# ACT CASE**STUDY**

## The Client and Their Challenge

We were contacted by the Practice Administrator of a large Orthopedic group in Central New Jersey. An industry expert referred us to her because the practice was using a PACS system at one of their sites and it was slowing their network down dramatically. The practice's existing IT group couldn't figure out what the problem was, so we were brought in to troubleshoot the situation.

### First Steps

Using our knowledge of the industry and the systems, we conducted a thorough review of their network and how it was interfacing with the PACS system. We made some changes to their configurations and processes and were able to minimize the drain that the PACS system was placing on their network. This solved their first problem.

### Additional Findings

During our review, we learned the existing team was doing all the basics technically correct—systems were backed up, firewalls were in place, and anti-virus software was configured correctly. However, there was no proactive IT planning occurring, nor had any HIPAA planning been done. More concerning was that during our initial walk-through we identified many HIPAA red flags that put patient data at risk daily.

Some examples of HIPAA violations include not using secure email, allowing multiple users to log in to systems using shared usernames and/or passwords, not having a rotating password policy, and not installing privacy screens on computers in public areas. In addition, employees were not participating in the required annual HIPAA training.

We were asked to address these risks.

### What We Did Next

We conducted a comprehensive Security Risk Analysis (SRA). Over the course of three days, we interviewed doctors and the practice administrator and performed a site assessment at each of their offices, reviewing every workstation and network configuration. We identified key areas of risk and vulnerability and put together a strategic plan that outlined how to remedy each area. Next, we partnered with one of our trusted vendors who specialize in HIPAA documentation in order to bring the practice into full compliance.

### A Measurable Impact

Within six months, the practice experienced increased productivity with their PACS system and as a result of our SRA, was able to achieve meaningful use. All of their employees were brought up-to-date on their HIPAA training and an annual plan was put in place to ensure continuity. In addition, a secure email system was set up, the network was configured and protected, and all data was set to automatically backup to a secure off-site location.

### How ACT Continues to Help

When our special engagement ended, the practice decided to engage us as their outsourced IT provider going forward. They became a Managed Service Contract client, which guarantees them around-the-clock attention and protection. Some of the things we do for them include:

- 24/7/365 monitoring
- Prioritized response time
- Remote help desk support
- On-site service calls, as needed
- Automated data backup
- Disaster recovery
- Patching and security updates for operating systems and managed software
- Proactively handle network alerts
- Regularly test backups to ensure they are functioning properly
- Conduct periodic IT planning meetings to ensure we are meeting all current and future needs

**Wondering if a Managed Service Contract is right for your practice? Give us a call to learn more— (973) 758-0500.**

A PROUD MEMBER OF

MGMA
Medical Group Management Association
New Jersey