adNET
Technology Management

A GUIDE TO SAFE IT PRACTICES IN A MEDICAL OFFICE:

EIGHT TECHNOLOGY PITFALLS THAT CAN UPEND YOUR MEDICAL PRACTICE—AND HOW TO AVOID THEM

The modern medical practice faces several challenges, not the least of which is establishing healthy information technology systems and methods. Phishing and other cybersecurity threats are becoming more and more prevalent in healthcare clinics, meaning careful and timely IT maintenance is vital to your practice's wellbeing.

However, managing a secure IT infrastructure can be overwhelming, especially because handling the obvious issues, such as security breaches, is only half the job. There are several IT issues that often go undetected in medical clinics because their staff consists of only one or two IT professionals who aren't trained to deal with healthcare-specific IT issues.

This guide aims to highlight eight IT pitfalls your clinic might face and the steps you can take to prevent them. If your practice faces IT problems that your in-house team can't cope with, it's time to call a healthcare-focused IT company to help you combat these pitfalls.

1. NOT HAVING A PLAN TO PROTECT AGAINST CYBER THREATS

Cybersecurity is a concern that faces all modern organizations, but in the healthcare industry failing to implement a cybersecurity protection plan means risking your patients' confidential information, and possibly putting you out of compliance with HIPAA. That means you stand to lose

IF YOUR PRACTICE FACES IT PROBLEMS THAT YOUR IN-HOUSE TEAM CAN'T COPE WITH, IT'S TIME TO CALL A HEALTHCARE-FOCUSED IT COMPANY TO HELP YOU COMBAT THESE PITFALLS.

Call us at (877) 264-2968 or email us at info@adnet.us.

For more information, visit our website at **www.adnet.us**.

more than just money in the event of a cybersecurity breach—you're looking at a myriad of legal consequences, too.

Additionally, by risking theft of data or the infiltration of an IT system, you put not only your reputation on the line, but also the survival of your entire medical practice. Lost data will inevitably lead to lost patients and could also mean that insurance companies refuse to pay claims.

Many cybercriminals are opportunistic. They will attempt to force a digital path into IT infrastructures and exploit any holes that exist. Whether it's through ransomware, phishing attacks, viruses, or malware infestation, they can quickly gain access to your network, unless you have adequate protection.

Ransomware attacks are especially prevalent and cause significant damage to healthcare facilities. Ransomware encrypts data or prevents staff from accessing certain files until a ransom is paid, and even if the ransom is paid regaining access to data is not guaranteed. In the meantime patient care is delayed or hindered.

2. SPENDING TOO MUCH TIME RESOLVING IT PROBLEMS

The modern facility uses a host of technologies that can streamline business processes and make managing your practice easier. However, when errors occur it can take considerable time to repair them. Having

1 | SUGGESTIONS:

Every medical practice should invest in an advanced cybersecurity plan that goes beyond simply installing anti-malware and antivirus software to avoid these dangers. Cybersecurity plans established by healthcare-savvy IT service providers such as adNET Technology Management are the best option because they ensure your data is protected from all forms of threats. They can strategize according to the needs of your specific medical practice to make certain your IT infrastructure is optimized for maximum security.

sufficient resources to regularly maintain software and hardware is crucial in order to reduce error and make sure your practice runs smoothly.

The challenge for medical practices is that many facilities have only a single IT specialist or a small handful of technicians at best. This short-handed staff is left to manage everything from data warehouses to servers, as well as make sure the Internet, databases, and other systems run efficiently. Some medical facilities do not have a dedicated IT team at all, and the job is left to administrative members who aren't well-trained to handle IT issues.

In cases such as these, limited IT personnel must focus their energy on more imminent security threats and don't have excess time to ensure the systems are being properly maintained and updated. Not to mention, a staff overwhelmed with IT issues must sacrifice valuable time they could be spending to care for patients.

Instead of sacrificing data safety and patient satisfaction, you can rely on a healthcare-focused IT team from adNET to manage your IT systems. Our teams, whether on-site or remote, can reduce maintenance and repair time. They can ensure that systems run efficiently and according to the needs of your practice. Through our managed IT services, our specialized team comes at the cost of as low as a single full-time employee. This leaves your team free to continue with their own jobs and gives you a streamlined healthcare facility where you can focus on patient care.

2 | SUGGESTIONS:

Instead of sacrificing data safety and patient satisfaction, you can rely on a healthcare-focused IT team from adNET to manage your IT systems. Our teams, whether on-site or remote, can reduce maintenance and repair time. They can ensure that systems run efficiently and according to the needs of your practice. Through our managed IT services, our specialized team comes at the cost of as low as a single full-time employee. This leaves your team free to continue with their own jobs and gives you a streamlined healthcare facility where you can focus on patient care.

3. FAILING TO IMPLEMENT THE NEWEST TECHNOLOGIES AND IT PRACTICES

Just as you and your medical staff strive to keep up with the latest medical procedures, it's important to stay up-to-date with the latest IT technologies to maximize security in your practice. The IT world is a rapidly advancing and evolving world. New technologies are quickly superseded by the next version, and every new iteration of a technology claims to be more robust and more secure than the last. It is vital that your IT staff understand what has changed and whether these changes benefit your practice.

3 | SUGGESTIONS:

As a medical professional, you shouldn't have to spend your valuable time researching the latest IT technologies instead of attending to patients. Using our managed healthcare IT services means that you can concentrate on patient care and rest assured that a team of technicians is already dedicating hours of research to finding the best technologies for your practice. It's their job to stay up-to-date on expanding technologies available to medical practices and to learn how to implement them.

4. BUYING THE WRONG EQUIPMENT

Right in line with not keeping up on the latest technology is the pitfall of purchasing the wrong equipment—equipment that is outdated, incompatible with your existing equipment, or just plain unnecessary. This is a common mistake in healthcare practices because medical personnel must often rely on a salesperson's claim that a piece of equipment will be useful to their business when in reality, it might not provide any value.

Even experienced IT technicians won't always know which upgrades to make to your IT infrastructure if they are not trained specifically in best practices for healthcare IT systems.

4 | SUGGESTIONS:

Our IT professionals at adNET have an invaluable combination of expertise in up-to-date IT services and an understanding of how to maintain IT infrastructures in the healthcare industry. Our healthcare-focused services help eliminate unnecessary costs by providing only the equipment that is useful to and compatible with your practice's IT infrastructure.

5. FALLING OUT OF COMPLIANCE WITH PCI DSS AND HIPAA REGULATIONS

The health sector is responsible for collecting, collating, and storing millions of pieces of data every year, and it is one industry that is most often hit by data loss.

In an effort to prevent data loss, your practice is required to adhere to regulations such as PCI DSS and HIPAA, so it's important that your systems remain consistently secure. If data does go missing and it is determined that your practice was negligent or culpable for the loss, it could result in a considerable fine and other punitive actions.

Further, these regulations are frequently updated, meaning that if you're not consistently updating your IT systems, you could fall out of PCI DSS and HIPAA compliance.

6. BELIEVING THAT DISASTERS ONLY HAPPEN TO OTHER CLINICS

Too many healthcare providers operate under the assumption that IT disasters only happen to other practices. But IT issues can be caused

5 | SUGGESTIONS

Using a managed IT service provider such as adNET not only affords you the benefit of not having to manage your IT systems yourself, but it also means that the IT service provider has accountability for your data protection practices. If errors occur in your systems, the IT service provider is responsible for maintaining the integrity and safety of your patient data. You can have greater peace of mind as a healthcare provider knowing that our technicians will do everything they can to secure your systems and ensure they are PCI DSS and HIPAA-compliant.

6 | SUGGESTIONS

It might seem impossible to prepare for every scenario, but that's what disaster and recovery plans are for. They identify potential threats to a system, and they put procedures, plans, and systems in place to prevent them. With recovery services such as data backup, recovery, and replication; image-based replications; and assured business continuance, you can rely on adNET to prepare your practice by making sure your data remains secure and accessible at all times.

by a number of factors that aren't always in your control. Human error is responsible for a good portion of a medical facility's downtime, but downtime can also be caused by anything from natural disasters such as floods and earthquakes to operational problems such as a power failure.

7. FAILING TO PLAN FOR THE FUTURE

It can be easy to get left behind with the many constant advancements being made to technology. With HIPAA and other regulations being frequently updated as well, it's important to ensure your systems are adaptable to future improvements. By planning for how to modify your IT infrastructure as technology undergoes updates and your practice grows, you can avoid pitfalls down the road.

8. NOT USING HEALTHCARE-EXPERIENCED IT SERVICES

As we've discussed, the healthcare industry has very specific requirements when it comes to IT infrastructure. Unless you have an extensive IT employee budget, it's likely you don't have all the in-house resources needed to meet those requirements. Using a managed healthcare IT service like adNET means that you can run a secure practice with minimal downtime. You can keep your systems virtually error-free and up-to-date on healthcare regulations, ensuring your time is dedicated to keeping your patients healthy and happy.

7 | SUGGESTIONS

Your systems, like your practice, need to be future-proof. They need to be agile. Our services allow you to create both a degree of redundancy in the system as well as budgets and plans to allow for future expansion.

8 | WHAT YOU CAN DO NOW:

At adNET Technology Management, we have a deep and sophisticated understanding of what your medical practice needs to manage its IT systems. Allow us to become your trusted partner in managing your IT systems and help you meet your business goals.

Contact adNET Technology Management today to speak with one of our IT service experts about how you can build a better, safer medical practice.

Call us at (877) 264-2968 or email us at info@adnet.us.

For more information, visit our website at **www.adnet.us**.