HealthyIT

The New York Practice Owners' Guide To IT Support Services And Fees

What You Should Expect To Pay For IT Support For Your Healthcare Practice

(And How To Get *Exactly* What You Need Without Unnecessary Extras, Hidden Fees And Bloated Contracts)

Read this guide and you'll discover:

- ✓ The 3 most common ways IT services companies charge for their services, and the pros and cons of each approach.
- ✓ A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- ✓ Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- ✓ How to make sure you know exactly what you're getting to avoid disappointment, frustration, and added costs later on that you didn't anticipate.
- ✓ 21 revealing questions to ask your IT support firm BEFORE giving them access to your computer network, e-mail, and data.

Provided as an educational service by:
Scott Sanford, President
Healthy IT, Inc.
320 Carleton Ave, Ste 1700
Central Islip, NY 11722
(631) 224-9450
www.MyHealthyIT.com

HealthyIT

Never Ask An IT Services Company, "What Do You Charge For Your Services?" Instead You Should Ask, **"What Will I *Get* For My *Money*?"**

From The Desk Of: Scott Sanford
President, Healthy IT

Dear Doctor,

If you are the owner of a healthcare practice in New York that is currently looking to outsource some or all of the IT support for your practice, this report contains important information that will be extremely valuable to you as you search for a competent firm you can **trust**.

My name is Scott Sanford, President of Healthy IT. We've been providing IT services to practices in the New York and Tri-State area for over 25 years now. You may not have heard of us before, but I'm sure you're familiar with one or more of the other healthcare practices who are clients of ours. A few of their comments are enclosed.

One of the most commons questions we get from new prospective clients calling our office is "What do you guys charge for your services?" Since this is such a common question — and a very important one to address — I decided to write this report for 3 reasons:

1. I wanted an easy way to answer this question and educate all prospective clients who come to us on the most common ways IT services companies package and price their services, and the pros and cons of each approach.

2. I wanted to bring to light a few "industry secrets" about IT service contracts and SLAs (service level agreements) that almost no practice owner thinks about, understands, or knows to ask about when evaluating IT service providers that can end up burning you with hidden fees and locking you into a long-term contract when they are unwilling or unable to deliver the quality of service you need.

3. I wanted to educate practice owners on how to pick the ***right*** IT services company for their specific situation, budget, and needs based on the ***VALUE*** the company can deliver, not just the price, high OR low.

In the end, my purpose is to help you make the most informed decision possible, so you end up working with someone who helps you solve your problems and accomplish what you want in a time frame, manner and budget that is right for you.

Dedicated to serving you,

Scott Sanford

About The Author
Scott Sanford – President & CEO

Scott Sanford has a penchant for working with Dentists. Why? He was going to be a dentist himself! While studying for the Dental Admissions Test, he discovered he enjoyed tinkering with the test bank software more than the actual studying! So, all signs seemed to point towards technology for dentists, and a career in Dental-focused technology began. Having worked as a Dental Assistant, Dental Repair Mechanic, and Systems Engineer provided Scott with a holistic view of what technology should be in a dental practice. For over 25 years, Healthy IT has been working with not only dentists, but also with a vast number of healthcare practices and organizations. Through Scott's extensive experience, he has gained a superior knowledge and familiarity with the unique software, hardware, and business processes needed to help healthcare offices operate effectively. This niche knowledge gives Healthy IT a huge competitive advantage.

Healthy IT began as an offshoot of S.T. Sanford Computer Consulting, Inc. We believed then, as we do now, that healthcare and dental professionals need superior, specialized IT support and services to best attend to their patients' needs. That's why we have dedicated ourselves to providing practices in New York and the tri-state area with all the technology solutions they need to improve patient experience and outcomes, while lowering their costs.

Scott has been featured in Dr. Steven Katz's book, *They Didn't Teach Us THAT in Dental School*. After many years of practicing as a dentist himself, Dr. Katz decided to venture out and create his own dental consulting company. Throughout his journey of helping other fellow dentists build up their practices to be successful and profitable, Dr. Katz wrote a book of his own experiences and thoughts on how you can grow a dental practice by working smarter, not harder. In Chapter 11, Dr. Katz speaks about the power of utilizing the full potential of computer systems, where Scott is recommended as the go-to technical solution architect for dental practices.

HealthyIT

Comparing Apples To Apples: The Predominant IT Service Models Explained

Before you can accurately compare the fees, services, and deliverables of one IT services company to another, you need to understand the three predominant service models most of these companies fit within. Some companies offer a blend of all three, while others are strict about offering only one service plan. The three predominant service models are:

- **Time and Materials**. In the industry, we call this "break-fix" services. Essentially, you pay an agreed-upon hourly rate for a technician to "fix" your problem when something "breaks." Under this model, you might be able to negotiate a discount based on buying a block of hours. The scope of work may be simply to resolve a specific problem (like removing a virus), or it may encompass a large project like a computer network upgrade or move that has a specific result and end date clarified. Some companies will offer staff augmentation and placement under this model as well.

- **Managed IT Services.** This is a model where the IT services company takes the role of your "IT department" and not only installs and supports all the devices and PCs that connect to your server(s), but also offers phone and on-site support, antivirus, security, backup, and a host of other services to monitor and maintain the health, speed, performance, and security of your computer network.

- **Software Vendor-Supplied IT Services.** Many software companies will offer IT support for their customers in the form of a help desk or remote support for an additional fee. However, these are typically scaled-back services, limited to troubleshooting their specific application and NOT your entire computer network and all the applications and devices connected to it. If your problem resides outside of their specific software or the server it's hosted on, they can't help you and will often refer you to "your IT department." While it's often a good idea to buy some basic-level support package with a critical software application you use to run your business, this is not enough to provide the full IT services and support most businesses need to stay up and running.

When looking to outsource your IT support, the two service models you are most likely to end up having to choose between are the "managed IT services" and "break-fix" models. Therefore, let's dive into the pros and cons of these two options, and then the typical fee structure for both.

Managed IT Services Vs. Break-Fix: Which Is The Better, More Cost-Effective Option?

You've probably heard the famous Benjamin Franklin quote, "An ounce of prevention is worth a pound of cure." I couldn't agree more — and that's why it's my sincere belief that some form of managed IT is essential for every healthcare practice.

In our company, we offer different plans to fit the needs of our clients. In some cases, where the practice is small, we might offer a very basic managed services plan to ensure the most essential

maintenance is done, then bill the client hourly for any support used. For our smallest clients, they often find this the most economical. But for some of our midsize to larger practices, we offer a fully managed approach where more comprehensive IT services are covered in a managed plan. By doing this, we can properly staff for their accounts and ensure they get the fast, responsive support and expertise they need.

The only time I would recommend a "time and materials" approach is when you already have a competent IT person or team proactively managing your computer network and simply have a specific IT project to complete that your current in-house IT team doesn't have the time or expertise to implement (such as migrating to a cloud-based solution, implementing a cyber security plan, etc.). Outside of that specific scenario, I do not think the break-fix approach is a good idea for general IT support for one very important, fundamental reason: you'll ultimately end up paying for a pound of "cure" for problems that could have easily been avoided with an "ounce" of prevention.

Why Regular Monitoring And Maintenance Is Critical For Today's Computer Networks

The fact of the matter is, computer networks absolutely, positively need ongoing maintenance and monitoring to stay secure. The ever-increasing dependency we have on IT systems and the data they hold — not to mention the *type* of data we're now saving digitally — has given rise to very smart and sophisticated cybercrime organizations and who work around the clock to do one thing: hack into your network to steal data or money or to hold you ransom.

As you may know, ransomware is at an all-time high because hackers make millions of tax-free dollars robbing one small business owner at a time. But that's not their only incentive.

Some will attempt to hack your network to gain access to bank accounts, credit cards, or passwords to rob you (and your patients). Some use your computer network to send spam using YOUR domain and servers, host pirated software and, of course, spread viruses. Some even do it just for the "fun" of it.

And don't think for a minute these cybercriminals are solo crooks working alone in a hoodie out of their basement. They are highly organized and well-run operations, employing *teams* of hackers who work together to scam as many people as they can. They use advanced software that scans millions of networks for vulnerabilities and use readily available data on the dark web of YOUR usernames, passwords, e-mail addresses, and other data to gain access.

Of course, this isn't the only IT danger you face. Other common "disasters" include rogue staff members, lost devices, hardware failures (still a BIG reason for data loss), fire and natural disasters, and a host of other issues that can interrupt or outright destroy your IT infrastructure and the data it holds. Then there's regulatory compliance for any business hosting or touching credit card or financial information, medical records, and even patient contact information such as e-mail addresses.

Preventing these problems and keeping your systems up and running (which is what managed IT services is all about) is a LOT less expensive and damaging to your practice than waiting until one of these things happens and then paying for emergency IT services to restore your systems to working order (break-fix).

Should You Just Hire A Full-Time IT Manager?

In most cases, it is not cost-effective for practices with under 50 employees to hire a full-time IT person for a couple of reasons.

First of all, no one IT person can know everything there is to know about IT support and cyber security. If your practice is big enough and growing fast enough to support a full-time IT lead, you probably need more than one guy. You need someone with help-desk expertise as well as a network engineer, a network administrator, a CIO (chief information officer), and a CISO (chief information security officer).

Therefore, even if you hire a full-time IT person, you may still need to supplement their position with co-managed IT support using an IT firm that can fill in the gaps and provide services and expertise they don't have. This is not a bad plan; what IS a bad plan is hiring one person and expecting them to know it all and do it all.

Second, finding and hiring good people is difficult; finding and hiring skilled IT people is incredibly difficult due to the skill shortage for IT. And if you're not technical, it's going to be very difficult for you to interview candidates and sift and sort through all the duds out there to find someone with good skills and experience. Because you're not technical, you might not know the right questions to ask during the interview process or the skills they need to do the job.

More often than not, the hard and soft costs of building an internal IT department for general IT support just don't provide the best return on investment for the average small to midsize practice. An internal IT department typically doesn't make sense until you have closer to 200 employees OR you have unique circumstances and need specialized skills, a developer, etc., but not for day-to-day IT support and maintenance.

Why "Break-Fix" Works Entirely In The Consultant's Favor, *Not* Yours

Under a "break-fix" model, there is a fundamental conflict of interests between you and your IT firm. The IT services company has no incentive to prevent problems, stabilize your computer network, or to resolve problems quickly because they are getting paid by the hour when things stop working; therefore, the risk of unforeseen circumstances, scope creep, learning curve inefficiencies, and outright incompetence are all shifted to YOU, the customer. Essentially, the more problems you have, the more they profit, which is precisely what you DON'T want.

Under this model, the IT consultant can take the liberty of assigning a junior (lower-paid) technician to work on your problem – one who may take two to three times as long to resolve an

issue that a more senior (and more expensive) technician may have resolved in a fraction of the time. There is no incentive to properly manage the time of that technician or their efficiency, and there is every reason for them to prolong the project and to find MORE problems than solutions. Of course, if they're ethical and want to keep you as a client, they *should* be doing everything possible to resolve your problems quickly and efficiently; however, that's akin to putting a German shepherd in charge of watching over the ham sandwiches. Not a good idea.

Second, it creates a management problem for you, the customer, who now has to keep track of the hours they've worked to make sure you aren't getting overbilled, and since you often have no way of really knowing if they've worked the hours they say they have, it creates a situation where you really, truly need to be able to trust they are being 100% ethical and honest AND tracking THEIR hours properly (not all do).

And finally, it makes budgeting for IT projects and expenses a nightmare since they may be zero one month and thousands the next.

What Should You Expect To Pay?

Important! Please note that the following price quotes are industry averages based on a recent IT industry survey conducted of over 750 different IT services firms. We are providing this information to give you a general idea of what most IT services firms charge and to help you understand the VAST DIFFERENCES in service contracts that you must be aware of before signing on the dotted line. Please understand that this does NOT reflect our pricing model or approach, which is simply to understand exactly what you want to accomplish FIRST and then customize a solution based on your specific needs, budget, and situation.

Hourly Break-Fix Fees: Most IT services companies selling break-fix services charge between $125 and $200 per hour with a one-hour minimum. In most cases, they will give you a discount of 5% to as much as 20% on their hourly rates if you purchase and pay for a block of hours in advance.

If they are quoting a **project**, the fees range widely based on the scope of work outlined. If you are hiring an IT consulting firm for a project, I would suggest you demand the following:

- **A very detailed scope of work that specifies what "success" is.** Make sure you detail what your expectations are in performance, workflow, costs, security, access, etc. The more detailed you can be, the better. Detailing your expectations up front will go a long way in avoiding miscommunications and additional fees later on to give you what you REALLY wanted.

- **A fixed budget and time frame for completion.** Agreeing to this up front aligns both your agenda and the consultant's. Be very wary of loose estimates that allow the consulting firm to bill you for "unforeseen" circumstances. The bottom line is this: it is your IT consulting firm's responsibility to be able to accurately assess your situation and quote a project based on their experience. You should not have to pick up the tab for a consultant underestimating a job or for their inefficiencies. A true professional knows

how to take into consideration those contingencies and bill accordingly.

Managed IT Services: Most managed IT services firms will quote you a MONTHLY fee based on the number of devices they need to maintain, back up and support. In New York, that fee is somewhere in the range of $200 to $500 per server, and approximately $25 to $50 per desktop.

If you hire an IT consultant and sign up for a managed IT services contract, here are some things that SHOULD be included (make sure you read your contract to validate this):

- Dark Web scans
- HIPAA Compliance
- Computer repairs, Hardware loaners and basic peripheral installation
- User security patches applied weekly, if not daily, for urgent and emerging threats
- Antivirus updates and monitoring
- Firewall updates and monitoring
- Backup monitoring and test restores
- Spyware detection and removal
- Monitoring disk space on workstations and servers
- Monitoring hardware for signs of failure
- Optimizing systems for maximum speed

The following services may **NOT be included** and will often be billed separately. This is not necessarily a "scam" or unethical UNLESS the managed IT services company tries to hide these fees when selling you a service agreement. Make sure you review your contract carefully to know what is and is NOT included!

- Hardware, such as new servers, PCs, laptops, etc.
- Software licenses
- On-site support – depends on what level of service was agreed on
- Projects

Warning! Beware of the gray areas of "all-inclusive" service contracts. In order to truly compare the "cost" of one managed IT services contract to another, you need to make sure you fully understand what IS and ISN'T included AND the "SLA" or "service level agreement" you are signing up for. It's VERY easy for one IT services provider to appear far less expensive than another UNTIL you look closely at what you are getting.

The following are 21 questions to ask your IT services provider that will clarify exactly what you're getting for the money. Some of these items may not be that important to you, while others (like response time, adequate insurance, and uptime guarantees) may be critical. Make sure you fully understand each of these items before deciding who the right provider is for you; then make sure you get this IN WRITING.

HealthyIT

21 Questions You Should Ask Your IT Services Company or Consultant Before Hiring Them For IT Support

Customer Service:

Q1: When I have an IT problem, how do I get support?

Our Answer: When a client has a problem, we "open a ticket" in our IT management system so we can properly assign, track, prioritize, document, and resolve client issues. However, some IT firms force you to log in to submit a ticket and won't allow you to call or e-mail them. This is for THEIR convenience, not yours. Trust me, this will become a giant inconvenience and thorn in your side. While a portal is a good option, it should never be your ONLY option for requesting support.

Also, make sure they HAVE a reliable system in place to keep track of client "tickets" and requests. If they don't, I can practically guarantee your requests will sometimes get overlooked, skipped, and forgotten.

Requesting support should also be EASY for you. So be sure to ask how you can submit a problem to their support desk for resolution. We make it easy. Calling, e-mailing, or submitting a ticket via our Support portal puts your IT issue on the fast track to getting resolved.

Q2: Do you offer after-hours support, and if so, what is the guaranteed response time?

Our Answer: Any good IT company will answer their phones LIVE (not voice mail or phone trees) and respond from 9:00 a.m. to 5:00 p.m. every weekday. But many business and practice owners work outside normal "9 to 5" hours and need IT support both nights and weekends. Not only can you reach our after-hours support any time and on Saturdays for emergencies, but we also GUARANTEE a response time of one hour or less for normal problems, and within 30 minutes for problems marked "emergency," such as a network being down or a critical problem that is significantly impacting your ability to work.

Q3: Do you have a written, guaranteed response time for working on resolving your problems?

Our Answer: Most IT firms offer a 60-minute or 30-minute response time to your call during normal business hours. Be very wary of someone who doesn't have a guaranteed response time IN WRITING – that's a sign they are too disorganized, understaffed, or too overwhelmed to handle your request. Our written, guaranteed response time is one hour or less. A good IT firm should also be able to show you statistics from their PSA (professional services automation) software, where all client problems (tickets) get responded to and tracked. Ask to see a report on average ticket response and resolution times.

Q4: Do they provide detailed invoices that clearly explain what you are paying for?

Our Answer: For the few things that we do not include in our managed services agreement, we provide detailed invoices that show what work was done, why and when, and by who, so you never have to guess what you are paying for. We also double-check our invoices for accuracy before they are sent to you.

Q5: Do you have a feedback system in place for your clients to provide "thumbs up" or "thumbs down" ratings on your service? If so, can I see those reports?

Our Answer: If they don't have this type of feedback system, they may be hiding their lousy customer service results. If they DO have one, ask to see the actual scores and reporting. That will tell you a lot about the quality of service they are providing. We are very proud of our positive client feedback scores and will be happy to show them to you.

IT Maintenance (Managed Services):

Q6: Do you offer true managed IT services and support?

Our Answer: You want to find an IT company that will proactively monitor for problems and perform routine maintenance on your IT systems. If they don't have the ability to do this, or they don't offer it, we strongly recommend you look somewhere else. Our remote network monitoring system watches over your network to constantly look for developing problems, security issues, and other problems so we can address them BEFORE they turn into bigger problems.

Q7: What is NOT included in your managed services agreement?

Our Answer: Another "gotcha" many IT companies fail to explain is what is NOT included in your monthly managed services agreement that will trigger an invoice. Their so-called "all you can eat" option is RARELY true – there are limitations to what's included, and you want to know what they are BEFORE you sign.

It's very common for projects to not be included, like a server upgrade, moving offices, adding new employees and, of course, the software and hardware you need to purchase.

But here's a question you need to ask: If you were hit with a costly ransomware attack, would the recovery be EXTRA or included in your contract? Recovering from a cyber-attack could take HOURS of high-level IT expertise. Who is going to eat that bill? Be sure you're clear on this before you sign, because surprising you with a big, fat bill is totally and completely unacceptable.

Other things to inquire about are:

- Do you offer a truly unlimited help desk? (Make sure you are not nickel-and-dimed for every call.)
- Does the service include support for cloud services such as Microsoft 365?
- Do you charge extra if you have to resolve a problem with a line-of-business application, Internet service provider, phone system, leased printer, etc.? (What you want is an IT company

that will own the problems and not point fingers. We are happy to call the vendor or software company on your behalf.)

- What about on-site support calls? Or support to remote offices?
- If our staff had to work remote (due to a shutdown, natural disaster, etc.), would you provide support on their home PCs, or would that trigger a bill?
- If we were to get ransomed or experience some other disaster (fire, flood, theft, tornado, hurricane, etc.), would rebuilding the network be included in the service plan or considered an extra project we would have to pay for? (Get this IN WRITING. Recovering from such a disaster could take hundreds of hours of time for your IT company's techs, so you want to know in advance how a situation like this will be handled before it happens.)

Our managed services agreement is completely transparent. Our coverage and terms are clearly defined, easy to understand, and make sense to our clients.

Q8: Is your help desk local or outsourced?

Our Answer: Be careful because smaller IT firms may outsource this critical function. As a result, you may get a tech who is not familiar with you, your network, previous problems, and personal preferences. Or worse, they may not be as qualified. This can be frustrating and lead to the same problems popping up over and over, longer resolution time, and you having to spend time educating the tech on your account.

Fortunately, we provide a dedicated technician to your account who will get to know you and your company, as well as your preferences and history. When you work with our local help desk technician, they'll be more capable of successfully resolving your IT issues and handling things the way you want.

Q9: How many engineers do you have on staff?

Our Answer: Be careful about hiring small, one-person IT firms that only has one technician, or that outsources this critical role. Everyone gets sick, has emergencies, goes on vacation, or takes a few days off from time to time. We have more than enough full-time techs on staff to cover in case one is unable to work.

ALSO: Ask how they will document fixes, changes, and credentials for your organization so if one tech is out or unavailable, another can step in and know your network settings, history, previous issues, etc., and how those issues were resolved. This is important or you'll be constantly frustrated with techs who are starting over to resolve a known issue or may screw up something because they don't understand or have a blueprint of your computer network.

Q10: Do you offer documentation of our network as part of the plan, and how does that work?

Our Answer: Network documentation is exactly what it sounds like: the practice of maintaining detailed technical records about the assets you own (computers, devices, software, directory structure, user profiles, passwords, etc.) and how your network is set up, backed up, and secured. Every IT

company should provide this to you in both written (paper) and electronic form at no additional cost and update it on a quarterly basis.

Why is this important? There are several reasons:

First, it shows professionalism and integrity in protecting YOU. No IT person or company should be the only holder of the keys to the kingdom. Because we document your network assets and passwords, you have a blueprint you can give to another IT person or company to take over if necessary.

Second, good documentation allows the engineers working on your account to resolve problems faster because they don't waste time fumbling their way around your network trying to find things and uncover accounts, hardware, software licenses, etc. Third, if you had to restore your network after a disaster, you'd have the blueprint to quickly put things back in place as they were.

Finally, and most important, if you ever need to switch IT providers, your replacement company will be able to take over quickly because the network has been documented properly.

All our clients receive this in written and electronic form at no additional cost. We also perform a quarterly update on this material and make sure certain key people from your organization have this information and know how to use it, giving you complete control over your network.

Side note: You should NEVER allow an IT person to have that much control over you and your company. If you get the sneaking suspicion that your current IT person is keeping this under their control as a means of job security, get rid of them (and we can help to make sure you don't suffer ANY ill effects). This is downright unethical and dangerous to your organization, so don't tolerate it!

Q11: Do you meet with your clients for Technology Business Reviews as part of your managed services agreement?

Our Answer: To us, there's nothing more important than face-to-face time with our clients. Therefore, we make it a priority to meet with all our clients at least semi-annually (sometimes more often) to provide a "technology review."

In these meetings, we provide you with the status updates of projects you're working on and of the health and security of your network. We also make recommendations for new equipment and upgrades you'll be needing soon or sometime in the near future. Our meetings with you are C-level discussions (not geek-fests) where we openly discuss your business goals, including your IT budget, critical projects, compliance issues, known problems, and cyber security best practices.

Our goal in these meetings is to help you improve operations, lower costs, increase efficiencies, and ensure your organizational productivity stays high. This is also your opportunity to give us feedback on how we're doing and discuss upcoming projects.

Q12: If I need or want to cancel my service with you, how does this happen and how do you offboard us?

Our Answer: Make sure you carefully review the cancellation clause in your agreement. Many IT firms hold their clients hostage with long-term contracts that contain hefty cancellation penalties and will even sue you if you refuse to pay.

We would never "force" a client to stay with us if they are unhappy for any reason; therefore, we make it easy to cancel your contract with us, with zero contention or fines. Our "easy out" agreements make us work that much harder to exceed your expectations every day, so we keep your business.

Cyber Security:

Q13: What training on cyber security does you and your in-house team have?

Our Answer: It's important that your IT firm have *some* type of *recent* training and / or certifications, and they should be able to answer this question, which demonstrates a dedication to learning and keeping up with the latest cyber security protections. If they don't have any, and they aren't investing in ongoing training for their engineers, that's a red flag. Some business owners won't invest in training and give this excuse: "What if I spend all this money in training my employees and then they leave us for another job?" Our response is, "What if you DON'T train them and they stay?"

You can feel confident that our in-house technicians have among the most advanced cyber security training available, including training through the cyber security program by Pax8/SentinelOne.

Q14: How do you lock down our staffs' PCs and devices to ensure they're not compromising our network?

Our Answer: As above, the question may get a bit technical. The key is that they HAVE an answer and don't hesitate to provide it. Some of the things they should mention are:

- 2FA (two-factor authentication)
- Advanced end-point protection, NOT just antivirus
- Auditing and logging

Because a combination of these lockdown strategies is essential to protecting your network and data, we employ ALL of these for our clients. Effective cyber security should never compromise between choosing this OR that. It should feature every weapon in your arsenal.

Q15: What cyber liability and errors and omissions insurance do you carry to protect me?

Our Answer: Here's something to ask about: if THEY cause a problem with your network that causes you to be down for hours or days, to lose data or get hacked, who's responsible? What if one of their technicians gets hurt at your office? Or damages your property while there?

In this litigious society we live in, you better make sure whomever you hire is adequately insured with both errors and omissions insurance, workers' compensation, and cyber liability – and don't be shy about asking them to send you the policy to review!

If you get hit with ransomware due to their negligence, someone has to pay for your lost sales, the recovery costs, and the interruption to your business operations. If they don't have insurance to cover YOUR losses of business interruption, they might not be able to pay, and you'll have to end up suing them to cover your costs. If sensitive patient data is compromised, who's responsible for paying the fines that you might incur and the lawsuits that could happen? No one is perfect, which is why you need them to carry adequate insurance.

True story: A few years ago, a company that shall not be named was slapped with several multimillion-dollar lawsuits from customers for bad behavior by their technicians. In some cases, their techs were accessing, copying, and distributing personal information they gained access to on customers' PCs and laptops brought in for repairs. In other cases, they lost a client's laptop (and subsequently all the data on it) and tried to cover it up. Bottom line, make sure the IT firm you are hiring has proper insurance to protect YOU.

Rest assured, we make it a priority to carry all the necessary insurance to protect you, including errors and omissions insurance, workers' comp, and cyber liability insurance. Simply ask, and we will be happy to show you a copy of our policy.

Q16: Who audits YOUR company's cyber security protocols and when was the last time they conducted an audit?

Our Answer: Nobody should proofread their own work, and every professional IT consulting firm will have an independent third party reviewing and evaluating their company for airtight cyber security practices.

There are many companies that offer this service, so who they use can vary (there's a number of good ones out there). If they don't have a professional cyber security auditing firm doing this for them on at least a quarterly basis, or if they tell you they get their peers to audit them, DO NOT hire them. That shows they are not taking cyber security seriously.

You can be confident in the effectiveness of our cyber security because we are audited annually.

Q17: Do you have a SOC and do you run it in-house or outsource it?

Our Answer: A SOC (pronounced "sock"), or security operations center, is a centralized department within a company to monitor and deal with security issues pertaining to a company's network.

What's tricky here is that some IT firms have the resources and ability to run a good SOC in-house (this is the minority of outsourced IT firms out there). Others cannot and outsource it because they know their limitations (not entirely a bad thing).

But the key thing to look for is that *they have one.* Less experienced IT consultants may monitor your network hardware, such as servers and workstations, for uptime and patches, but they might not provide security monitoring. This is particularly important if you host sensitive data (financial information, medical records, credit cards, etc.) and fall under regulatory compliance for data protection.

Rest assured, we do have the best-in-class outsourced SOC to provide proactive security monitoring for our clients to better prevent a network violation or data breach.

Backups And Disaster Recovery:

Q18: Can you provide a timeline of how long it will take to get my network back up and running in the event of a disaster?

Our Answer: There are two aspects to backing up your data that most business owners aren't aware of. The first is "fail over" and the other is "fail back." For example, if you get a flat tire, you will fail over by putting on the spare tire to get to a service station where you can fail back to a new or repaired tire.

If you were to have a disaster that wiped out your data and network – be it a ransomware attack or natural disaster – you want to make sure you have a fail-over solution in place so your staff members could continue to work with as little interruption as possible. This fail-over should be in the cloud and locked down separately to avoid ransomware from infecting the backups, as well as the physical servers and workstations.

But, at some point, you need to fail back to your on-premise network, and that's a process that could take days or even weeks. If the backups aren't done correctly, you might not be able to get it back at all.

So, one of the key areas you want to discuss with your next IT consultant or firm is how they handle both data backup AND disaster recovery. They should have a plan in place and be able to explain the process for the emergency fail-over, as well as the process for restoring your network and data with a timeline.

In this day and age, regardless of natural disaster, equipment failure, or any other issue, your business should ALWAYS be able to be operational with its data within six to eight hours or less, and critical operations should be failed over immediately.

We understand how important your data is and how getting your team up and running quickly is essential to your practice's success. Therefore, in the event of any disaster, we can confidently get your network back up and running in 8 hours or less.

Q19: Do you INSIST on doing periodic test restores of my backups to make sure the data is not corrupt and could be restored in the event of a disaster?

Our Answer: A great IT consultant will place eyes on your backup systems every single day to ensure that backups are actually occurring, and without failures. However, in addition to this, your IT company should perform a monthly randomized "fire drill" test restore of some of your files from backups to make sure your data CAN be recovered in the event of an emergency. After all, the WORST time to "test" a backup is when you desperately need it.

If you don't feel comfortable asking your current IT company to test your backup OR if you have concerns and want to see proof yourself, just conduct this little test: Copy three unimportant files onto a thumb drive (so you don't lose them) and delete them from your server. Make sure one was newly created that same day, one was created a week earlier and the last a month earlier. Then call your IT company and let them know you've lost three important documents and need them restored from backups as soon as possible. They should be able to do this easily and quickly. If not, you have a problem that needs to be addressed immediately!

Verifying your backups daily and testing them on a regular basis is a cornerstone of a successful overall IT strategy. These are the lengths we go to for all our clients, including multiple random "fire drill" test restores to ensure ALL your files are safe because they are always backed up.

TIP: Ask your IT provider about the "3-2-2" rule of backups, which has evolved from the "3-2-1" rule. The 3-2-1 rule is that you should have three copies of your data: your working copy, plus two additional copies on different media (tape and cloud), with at least one being off-site for recovery. That rule was developed when tape backups were necessary because cloud backups hadn't evolved to where they are today. Today, there are more sophisticated cloud backups and BDR (backup and disaster recovery) devices. Therefore, we recommend you have three copies of your data: two copies stored locally, but on different devices, and two copies stored offsite (one copy in a remote location, and one copy to the cloud).

Q20: If I were to experience a location disaster, pandemic shutdown, or other disaster that prevented me from being in the office, how would you enable me and my staff members to work from a remote location?

Our Answer: If Covid taught us anything, it's that work-interrupting disasters CAN and DO happen when you least expect them. Fires, floods, hurricanes, and tornadoes can wipe out an entire building or location. Covid forced everyone into lockdown, and it could happen again.

We could experience a terrorist attack, civil unrest, or riots that could shut down entire cities and streets, making it physically impossible to get into a building. Who knows what could be coming down the pike? Hopefully NONE of this will happen, but sadly it could.

That's why you want to ask your prospective IT consultant how quickly they were able to get their clients working remote (and securely) when Covid shut everything down. Ask to talk to a few of their clients about how the process went.

Here's how we handled our clients' needs when it seemed everyone needed to work remote, get laptops, and implement security measures almost overnight. We quickly implemented VPN access and remote desktop connectivity where appropriate. For some, Microsoft Office 365 was all that was needed, but in the end, our ability to quickly address needs and provide a smooth and cost-effective solution was most valuable to our clients.

Q21: Show me your process and documentation for onboarding me as a new client.

Our Answer: The reason for asking this question is to see if they HAVE SOMETHING in place. A plan, a procedure, a process. Don't take their word for it. Ask to SEE it in writing. What's important

here is that they can produce some type of process. Further, they should be able to explain how their process works.

One thing you will need to discuss in detail is how they are going to take over from the current IT company – particularly if the current company is hostile. It's disturbing to me how many IT companies or people will become bitter and resentful over being fired and will do things to screw up your security and create problems for the new company as a childish way of getting revenge. (Sadly, it's more common than you think.) A good IT company will have a process in place for handling this.

If you consider us as your next IT services firm, we will gladly share our new client onboarding process and documentation. I think you'll be impressed.

Other Things To Notice And Look For:

Are they good at answering your questions in terms you can understand and not in arrogant, confusing "geek-speak"?

Good IT companies won't confuse you with techno-mumbo-jumbo, and they certainly shouldn't make you feel stupid for asking questions. All great consultants have the "heart of a teacher" and will take time to answer your questions and explain everything in simple terms. As you interact with them in the evaluation process, watch for this.

Our technicians are trained to take time to answer your questions and explain everything in simple terms. Just look at what this one client had to say:

"My experience with Healthy IT has been superb. I have used other computer support companies over the years, but Healthy IT is by far the best. I have called before hours and have not left a message because I felt that it was too early. Right after stepping into the office, Joey saw my missed call and called me, despite the time, to follow up. He then proceeded to resolve my slow-running computer issue quickly and courteously, *with a clear explanation of the cause*. I appreciate their technical excellence, but just as important, is their reliability and *true customer focus*. After they fix my technical issues, they then *follow-up a few days later* to make sure everything is running smoothly. When they are planning on working on-site, they call when they are on their way. It is a true pleasure to work with such a friendly staff and with a team that can explain anything to someone that has no idea about the workings of a computer. I recommend Healthy IT to everyone that asks about an IT company."
Gold Coast Smiles, PLLC

Do they and their technicians present themselves as true professionals when they are in your office? Do they dress professionally and show up on time?

If you'd be embarrassed if YOUR clients saw your IT consultant behind your desk, that should be a big red flag.

How you do anything is how you do everything, so if they cannot show up on time for appointments, are sloppy with paperwork, show up unprepared, forget your requests, and seem

disorganized in the meeting, how can you expect them to be 100% on point with your IT? You can't. Look for someone else.

Our technicians are true professionals who you would be proud to have in your office. They dress professionally and show up on time, and if they cannot be there on time (for some odd, unforeseen reason), we always notify the client immediately. We believe these are minimum requirements for delivering a professional service.

Do they have expertise in helping clients similar to you?

Do they understand how your practice operates the healthcare-specific applications you depend on? Are they familiar with how you communicate, get paid, service your patients, and run your practice? We have over 300 healthcare clients. The reason we work well with them is because Scott, the CEO of Healthy IT, has extensive knowledge on healthcare-specific applications and software; after all, he used to be a direct care provider in the dental industry himself. Here's what two clients had to say:

Using Healthy IT Will Make You Feel More Secure With Your Technology!

Healthy IT is very knowledgeable regarding the dental software which seems to be the most troublesome aspect of our system. They are able to integrate and get the various pieces to communicate properly, whether it's the digital x-rays, intraoral cameras, practice management or patient communications.

Steve Levy, DMD
Progressive Dentistry

Unparalleled Knowledge of Dental Software and Technology

With Healthy IT, we are working with a company whose response time is excellent. Access to someone for help is amazing! A phone call or email elicits immediate response and a follow-up. Healthy IT has given my dental office the security of knowing that we're not alone and that they understand the frustration that comes with a glitch. Healthy IT is big enough to handle a multitude of offices and problems, yet small enough to personalize the relationship with each office they serve.

Stephen D. Fluger, DDS
Island East Dental Group

A Final Word And Free Offer To Engage With Us

I hope you have found this guide helpful in shedding some light on what to look for when hiring a professional firm to outsource your IT support to. As I stated in the opening of this report, my purpose in providing this information was to help you make an informed decision and avoid getting burned by incompetent or unethical firms luring you in with cheap prices.

The next step is simple: call my office at 631-224-9450 ext. 111 and reference this letter to schedule a brief 10- to 15-minute initial consultation with me.

On this call we can discuss your unique situation and any concerns you have and, of course, answer any questions you have about us. If you feel comfortable moving ahead, we'll schedule a convenient time to conduct our proprietary 57-Point IT Systems Assessment.

This Assessment can be conducted 100% remote or on-site – whichever you would prefer - with or without your current IT company or department knowing (we can give you the full details on our initial consultation call). **At the end of the Assessment, you'll know:**

- Where you are overpaying (or getting underserved) for the services and support you are currently getting from your current IT company or team.
- Whether or not your systems and data are *truly* secured from hackers and ransomware, and where you are partially or totally exposed.
- If your data is *actually* being backed up in a manner that would allow you to recover it quickly in the event of an emergency or ransomware attack.
- Where you are unknowingly violating HIPAA regulations and requirements.
- How you could lower the overall costs of IT while improving communication, security, and performance, as well as the productivity of your staff members.

Fresh eyes see things that others cannot – so, at a minimum, our free assessment is a completely cost- and risk-free way to get a credible third-party validation of the security, stability, and efficiency of your IT systems.

To Schedule Your Initial Phone Consultation:

www.myhealthyit.com/free-consultation

Call: 631-224-9450 Ext. 111

With appreciation,

Scott Sanford, President
Healthy IT, Inc.
Phone: 631-2249450 ext. 111
E-mail: help@myhealthyit.com
Web: www.myhealthyit.com

HealthyIT

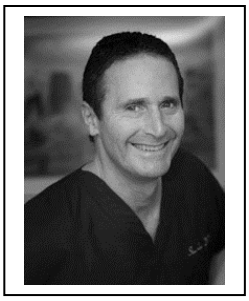
See What Other Practice Owners Are Saying:

Unparalleled Knowledge Of Dental Software And Technology

With Healthy IT, we are working with a company whose response time is excellent. Access to someone for help is amazing! A phone call or email elicits immediate response and a follow-up. Healthy IT has given my office the security of knowing that we're not alone and that they understand the frustration that comes with a glitch. Healthy IT is big enough to handle a multitude of offices and problems, yet small enough to personalize the relationship with each office they serve.

Stephen D. Fluger, DMD – Island East Dental Group

Trustworthy, Proactive And Always Available



I've used Scott Sanford, owner of Healthy IT, for years and have always valued his honesty, the quality of work him team provides, and knowing that they're always available should a computer problem arise. They are proactive and extremely knowledgeable. When it came to building my new dental office Scott was the only one I trusted to do the IT. A major plus: He's a really nice guy!

Steven M. Levy, DMD – Progressive Dentistry

Happy Client For Over 2 Decades

I have been dealing with Scott Sanford and Healthy IT for over 20 years. Scott and his crew are quick to respond, highly trained and very professional. When my patients call I am there for them…When I call Healthy IT they are there for me!

Howard S. Glazer, DDS – Family & Aesthetic Dentistry

HealthyIT

The Top 7 Reasons Why You'll Want To Outsource Your IT Support To Us:

1. **We Respond Within 5 Minutes Or Less.** The average amount of time it takes for one of our clients to get on the phone with a technician who can start working on resolving their problem is 3.5 minutes. We know you're busy and have made a sincere commitment to making sure your computer problems get fixed FAST. And since most repairs can be done remotely using our secure management tools, you don't have to wait around for a technician to show up.

2. **No Geek-Speak.** You deserve to get answers to your questions in PLAIN ENGLISH, not in confusing technical terms. Our technicians will also not talk down to you or make you feel stupid because you don't understand how all this "technology" works. That's our job!

3. **100% No-Small-Print Satisfaction Guarantee.** Quite simply, if you are not happy with our work, we'll do whatever it takes to make it right to YOUR standards without charging you for it. And if we can't make it right, the service is free.

4. **All Projects Are Completed On Time And On Budget.** When you hire us to complete a project for you, we won't nickel-and-dime you with unforeseen or unexpected charges or delays. We guarantee to deliver precisely what we promised to deliver, on time and on budget, with no excuses.

5. **Lower Costs, Waste And Complexity With Cloud Solutions.** By utilizing cloud computing and other advanced technologies, we can eliminate the cost, complexity, and problems of managing your own in-house server while giving you more freedom, lowered costs, tighter security, and instant disaster recovery.

6. **We Won't Hold You Hostage.** Many IT companies do NOT provide their clients with simple and easy-to-understand documentation that outlines key network resources, passwords, licenses, etc. By keeping that to themselves, IT companies hold their clients "hostage" to scare them away from hiring someone else. This is both unethical and unprofessional. As a client of ours, we'll provide you with full, written documentation of your network and all the resources, software licenses, passwords, hardware, etc., in simple terms so YOU can understand it. We keep our clients by delivering exceptional service — not by keeping them in the dark.

7. **Peace Of Mind.** Because we monitor all of our managed clients' networks 24/7/365, you never have to worry that a virus has spread, a hacker has broken in, or a backup has failed to perform. We watch over your entire network, taking the management and hassle of maintaining it off your hands. This frees you to focus on your patients and running your practice, not on your IT systems, security, and backups.