The IT Security Crisis For Medical Practices

NEW And Critical Changes To IT Security, Insurance Coverage, And HIPAA Compliance That Will Put Your Practice At Serious Financial Risk If Not Addressed This Year

Discover what the vast majority of small medical practices and covered entities don't know and haven't been told about changes to cyber security risks, insurance and HIPAA compliance laws that are allowing them to operate at **UNDER APPRECIATED RISK** for a crippling cyberattack and subsequent costs, lawsuits and fines – and what to do about it now.

Provided By: Tech Advisors, Inc.
Author: Konrad Martin
Boston, MA | Providence, RI | Marlborough, MA | West Palm Beach, FL
www.tech-adv.com
508-356-5565

About The Author

Konrad Martin is the CEO of Tech Advisors, a firm he founded in 2002 with his twin brother Kevin. Tech Advisors is a complete technology solution provider, 100% committed to seeing that business owners have the most reliable, professional IT service. Under Konrad's leadership, the firm has achieved steady growth and expansion of services offered including cybersecurity, HIPAA compliance, cloud computing and more to growing businesses across a wide range of industries, including medical practices of varying specialties.

Specifically, Tech Advisors works in partnership with medical practice executives, focusing on the technological needs of the practice – such as coordinating with Electronic Medical Records (EMR) companies, devising specific policies and procedures for how work in the IT environment while being mindful of HIPAA and regulatory compliance issues, and training providers to be cybersecurity aware – so they can focus on the practice itself. Tech Advisors understands the need for precise, effective and quick responses, and has a proven track record of expediency in solving technological issues.

Tech Advisors was named one of the world's premier managed service providers in the prestigious 2022 and 2021 Channel Futures MSP 501 rankings, as well as the Top 250 MSSP (Managed Security Service Providers) in 2021. Originally focused on the greater Boston area, the company has grown to offer services throughout the East Coast, and maintains offices in Boston, MA, Providence, RI, Marlborough, MA, and Palm Beach, FL.

Tech Advisors has combined experience of over 100 years of Cyber Security, IT Support, and Compliance knowledge and experience across its team of dedicated experts. Tech Advisors' team includes a robust, competent and responsive 3 tier team of Support Engineers and a dedicated Sales and Client Support team, which is always expanding to respond to the rapidly growing market demand.

A nationally recognized authority in the field of cybersecurity, Konrad was recently featured in the documentary, "Cyber Crime 2: The Dark Web Uncovered." The film chronicles the growing plague of cybercrime, where billions of dollars are stolen or lost each year, destroying businesses and lives. Konrad and nine other national cybersecurity experts were selected for the film, in which they explore the psychology and techniques of cybercrime and offer tips on how to avoid becoming a victim.

Konrad is also the co-author of *Cyber Storm*, an Amazon #1 best seller, as well as the author of *Hacked! How to Protect Your Business from the Fines, Lawsuits, Customer Loss and PR Nightmare Resulting from Data Breach and Cybercrime*, which offers strategies on staying one step ahead of cybercriminals, and *The I.T. Factor*, a comprehensive guide for the small business owner who seeks to find a professional, competent IT provider. Konrad has authored additional cybersecurity articles for a number of regional and national magazines, and was featured in *MSP Success Magazine's* Spring 2021 special edition with his article, "The CPA Turned IT Consultant Every CPA Firm Wants to Know."

Konrad uses his publications and other platforms to educate audiences on the field of cybersecurity and the reality that cybercrime is a sophisticated and organized industry. He believes strongly that education and empathy are critical, and that teams that are unified and knowledgeable are the best way to fight against the growing danger.

Before founding Tech Advisors, Konrad worked as a CPA; this background gives Konrad an understanding and appreciation of the financial side of technology, and he enjoys helping Tech Advisors' clients connect the value of a well-managed IT infrastructure with business efficiency and profitability. His background also led him to become a trusted advisor to the Massachusetts Society of CPAs; he wrote the WISP (Written Information Security Plan) for their organization and its hundreds of members.

TECH ADVISORS
IT Support and Cybersecurity Management

The Truth Nobody Is Telling You About IT Security And HIPAA Compliance

All of the hard work, investments and time you've put into growing your practice is at HIGH risk due to the false information and half-truths you've been told by high-paid HIPAA consultants, IT companies and even your insurance provider.

You *think* your IT company or person has your network protected. You *think* you're HIPAA compliant (or at least good enough). You *think* your insurance company will cover your losses and expenses if a breach occurs. You *think* your staff is being smart and not putting you at risk because they log into a HIPAA compliant or supposedly secure portal. You *think* your bank, credit card processing company or software vendor assumes all the risk for the payments you take and credit card processing. And you *think* that because you're small, nobody wants to target you.

Worst of all, you *think* a data breach would be minor inconvenience with very little negative effects or costs. And two years ago, you might have been right…

But today, ALL of these assumptions are wildly inaccurate – and if you're still operating on any of these, you are putting your practice at risk for serious financial damages with long-reaching negative implications. Consider this report is your wake-up call. There have been significant changes over the last few years in cyber-attacks, HIPAA compliance, what insurance will cover (and what's necessary to make sure your claim is not denied) and IT protections. The plan you put in place a year or two ago to deal with all of this is no longer viable.

We can practically guarantee what you've been told about keeping your practice secure from hackers is either wildly inaccurate or insufficient and incomplete, putting you in a situation of under-appreciated risk; and when a breach happens, those who sold you their "HIPAA compliant" solution will be nowhere to be found, accepting no responsibility, **leaving you to face it all on your own and paying out of your pocket.**

You don't want to be blindsided by a breach, then discover how much this can negatively impact you, and find yourself saying, "Why wasn't I told THAT?"

To be clear, this is not just about meeting a government standard (HIPAA). This is about making sure you completely understand the risks associated with a cyber-attack, IT failure or employee mistake and the costs, consequences and damage it will do to your practice.

That's why we wrote this report. Over the last few years, we've discovered that ZERO of the medical clients and other covered entities we've assessed before becoming clients are even

close to being prepared for a security incident, much less pass a HIPAA compliance audit. **Not a single one**.

All of them were operating under the incorrect assumption that 1) they were "secure enough" and 2) grossly underestimated the costs and wide-reaching negative impact a breach would have. Their trusted team of "experts" who are supposed to be informing them and protecting them are FAILING to do their job. You are very likely in the same situation.

This means if you were to experience a breach (and it's getting more and more likely you will) your staff would instantly be hit with a crushing workload of clean up to recover from the breach, time spent dealing with auditors, the FBI and attorneys who will overwhelm them with things they need for their investigation. You would also be financially devastated by the fines, emergency IT services, legal fees and services you would be forced to buy just to get back up and running. **Worse yet, there is a very good chance your insurance claim could be denied or not fully paid out due to your failure to do the things we've outlined in this report**.

This is NOT a subject you want to take lightly or "assume" you have handled. HIPAA compliance and IT systems security should NOT be entirely abdicated to your Practice Administrator, IT department or company. It should not be assumed that because your software company is "HIPAA compliant" that you are – and that you are protected from a cyber-attack. YOU need to get the facts about what it means to be "Willfully Neglectful" and make choices about what risks you are willing to take, if any, because it will be your practice's reputation and your financial responsibility should a breach happen.

Bottom line, medical practices are the #1 target for cyber criminals for reasons we'll discuss in this report – and you have almost certainly NOT been given a plan that is 1) complete, 2) practical and 3) affordable. Your parachute is full of holes, and you are completely without a backup chute that will deploy.

QUESTION: When was the last time your current IT company had THIS conversation with you? What HAVE they told you about these new threats? If they have been silent, then I would urge you to read this report in full and act on the information urgently.

"A Breach Won't Happen To My Practice…We're Too Small. My Staff Is Too Smart. We're Good," You Say?

Don't think you're in danger because you're a "small" practice and don't have anything a hacker would want? That you have "good" people who know better than to click on a bad e-mail or make a mistake? That it won't happen to you?

That's EXACTLY what cybercriminals are counting on you to believe.

It makes you easy prey because you put ZERO protections in place, or grossly inadequate ones. In fact, SMALL medical practices are the target because you're infinitely easier to compromise. Hackers are unethical, but *not* stupid.

You have a bread bag twist tie locking the gate to a veritable goldmine of prize data (medical records) that can be sold for millions of dollars on the Dark Web. Let's be clear: You are dealing with highly sophisticated cyber criminals who can and have outsmarted extremely competent IT teams working for large organizations and government entities. You and your staff are NOT above making a mistake or being duped.

Further, most of the small medical practices that get breached are not "handpicked" by hackers – that's not how they operate. They run grand scale operations using automated software that works 24/7/365 to scan the web to indiscriminately target as many victims as they can. Like commercial fishing boats, they cast wide nets and set baited traps – and yes, medical practices DO get targeted and DO get breached every day – **and the attacks are escalating**.

According to HIPAAJournal.com, in 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 4 years and the rate has doubled. **In 2021, an average of 1.95 healthcare data breaches of 500 or more records were reported each day**.

You just don't hear about these breaches because the news wants to report on BIG attacks, or it's kept quiet by the practice for fear of attracting bad PR, lawsuits and data-breach fines out of sheer embarrassment.

But make no mistake – medical practices are being compromised daily, and clinging to the smug ignorance of "That won't happen to me" is an absolute surefire way to leave yourself wide open to these attacks. And if you get breached, you WILL be fined and questioned about what you did to protect patient data. Unlike other businesses, you have a legal obligation to protect that information, and you would face financial consequences IF you shrugged this off, made the assumption you are "good" or abdicated this security responsibility entirely to your staff.

If a real estate firm gets hacked and sued for exposing sensitive data, they can argue they didn't know they should have been more careful with security. But a doctor trying to make that argument won't win. **Saying you "didn't know" is not even a reasonable excuse given the medical profession has been operating under HIPAA for over 30 years now**. No judge is going to buy that excuse. You HAVE been warned. You HAVE been told and you should know better.

Are you 100% sure you're "too small" to deal with a hacker who exposes your patients' medical records? Are you "too small" to worry about paying the fines and costs that you will incur? According to Osterman Research, the AVERAGE ransomware demand is now $84,000 (source: MSSP Alert) – and that does not include fines, lawsuits, emergency IT services or lost business.

It's also estimated that small businesses lose about $100,000 in revenue per ransomware incident and over 25 hours of downtime – add that to the minimum fine for willful violations of HIPAA of $50,000 for the first violation, and up to $250,000 or more for repeat violations. Of course, $150,000 isn't the end of the world, is it? But are you okay to shrug this off? To take the chance?

Larger hospitals have extensive staff and the ability to invest in sophisticated technology to protect them, as well as lawyers and IT personnel on staff to address and respond should an incident occur. **That's NOT the case for you, the small practice**. You don't have such resources or the funding to afford them; therefore, the LAST thing you need is to be woefully unprepared for an inevitable breach or HIPAA violation, which will undoubtedly be made worse by some ambulance-chasing attorney who convinces even one of your patients they've been significantly harmed by your lack of compliance.

Covid has already taken its toll on the medical field. Physicians from around the country have struggled financially through no fault of their own – and despite the fact we're getting back to some type of normalcy, many providers are still recovering from losses and can NOT afford another significant hit like a HIPAA violation or breach would deliver.

How Bad Can It Be?
My Insurance Will Cover Me, Won't It?

Insurance companies are in the business to make money, NOT pay out policy claims.

A few years ago, cyber insurance carriers were keeping 70% of premiums as profit and only paying out 30% in claims. Fast forward to today and those figures are turned upside-down, causing carriers to make drastic changes in how cyber liability insurance is acquired and coverages are paid.

For starters, getting even a basic cyber liability policy today may require you to prove you have certain security measures in place, such as multi-factor authentication, password management, endpoint protection and tested and proved data backup solutions. These carriers want to see phishing training and cyber security awareness training in place, and some will want to see a WISP and/or a Business Continuity Plan from your organization. Depending on the carrier, your specific situation and the coverage you're seeking, the list can be longer.

But the biggest area of RISK that is likely being overlooked in your practice is the actual enforcement of critical security protocols required for insurance coverage and compliance. Insurance carriers can (and will) deny payment of your claim if you failed to actually implement the security measures required to secure coverage. When a breach happens, they will investigate how it happened and whether or not you were negligent before paying out on your claim.

You cannot say, "I thought my IT company was doing this!" as a defense. Your IT company will argue they were not involved in the procurement of the policy and did not warranty

your security (none will; check out your contract with them). They might show evidence of you refusing to purchase advanced security services from them to further distance them from any responsibility. And if you haven't been documenting the steps you've taken to secure private health records and PII (personally identifiable information) to prove that you were not "willfully negligent," **this gigantic expensive nightmare will land squarely on your shoulders**.

Exactly How Can Your Practice Be Damaged By Cybercrime And A Known Data Breach Of Patient Data?
Let Us Count The Ways:

1. **Loss Of Patients And Revenue:** If you are breached, you will be forced to notify your patients that you exposed their private information to hackers.

   Do you think all of your patients will rally around you? Have sympathy? News like this travels fast on social media. They will demand answers: HAVE YOU BEEN RESPONSIBLE in putting in place the protections outlined in this report, or will you have to tell your patients, "Sorry, we exposed your private medical information and financial data to criminals because we didn't think it would happen to us," or "We didn't want to invest in HIPAA compliance because we're small." That will not be sufficient to pacify your patients, and the trust you've worked so hard to build will be destroyed.

   It's true that some of your patients will be understanding. Some won't even care. But you can bet there will be some small percentage of your patients who become irate, reporting you to the Department of Health and Human Services Office for Civil Rights (OCR) and if applicable, to their 3rd party payer, including Medicare – *and it only takes ONE lawsuit to make your life miserable*. Worse case, they find an attorney who will take their case for invasion of privacy or for negligence of doctor-patient confidentiality. Even if they don't have a case and cannot prove damages, do you really need that headache?

   At the very least they will find another provider and will be sure to tell their friends and family how you exposed their private medical and financial information to criminals. Let's say it's only 20%; but can you afford to lose 20% of your patients overnight, along with their friends and family members who are (or could be) potential patients?

2. **Legal Fees, HIPAA Fines, Lawsuits:**

   When a breach happens, you will incur emergency IT support and services that can quickly run into thousands of dollars. It's also very likely you'll want to retain an attorney. Even if you somehow avoid a fine for non-compliance to HIPAA standards, there will be costs and hours upon hours of time invested into gathering the mountain of data the auditors will want to see. You and your team are already busy, overburdened staff will be forced to take time to respond. You will be questioned and investigated and will likely want to retain the services of an attorney to represent you against the auditors. None of this will be cheap and

it will have a lasting, negative effect on your practice.

3. **Cost After Cost:**

According to the IBM Cost Of Data Breach Report, the cost of a data breach was highest in the healthcare industry. It's estimated that the cost per lost or stolen record is between $150 to $225 per record compromised, after factoring in IT recovery costs, lost revenue, downtime, fines, legal fees, etc. How many client records do you have? Employees? Multiply that by $150 on the conservative side and you'll start to get a sense of the potential costs to your practice. **Here are just a few of the costs you might not have considered**:

- Paying the ransom to get your data back. Sophos, a well-known, leading cybersecurity company, recently published the "State Of Ransomware In Healthcare" report. This report revealed that healthcare was the most likely sector to pay a ransom, with just over 60 percent of respondents who experienced encryption admitted to paying the ransom, compared to a cross-sector average of 46 percent.

- Credit and ID theft monitoring for EVERY patient impacted at a cost of $10 to $30 per record.

- Notification costs of having to print and mail patients about the breach.

- Costs of your staff having to deal with a tsunami of paperwork, phone calls, tasks and projects to clean up the mess and deal with the auditors, which takes them away from productive work you hired them to do.

- The fees and IT costs to remediate all of your insurance company's forensic findings and re-establishing valid BAA agreements.

- If the breach involves a computer that transmits or hosts credit card data:
  - ✓ Fess of $500,000 per incident for being PCI non-compliant
  - ✓ Increased audit requirements
  - ✓ Potentially increase credit card processing fees
  - ✓ Potential for a company wide shut down of credit card activity by your merchant bank, requiring you to find another processor
  - ✓ Cost of printing and postage for notification mailing that is separate from the medical record notification

It's Not The Government Auditors That You Have To Worry About, But This…

Complaints filed for HIPAA violations primarily come from two sources: 1. An actual cyberattack happening, or 2. Whistleblowers *inside* the organization.

More specifically, disgruntled patients and employees.

They can be financially rewarded for reporting YOU and be protected under a Safe Harbor law. Ambulance chasing attorneys know this and are advertising to take whistleblower cases on Google (just do a quick search for "Medicaid fraud whistleblower reward" and look at the ads that come up from law firms). There's even a website, www.CorporateWhistleBlower.com that promotes, "Get Rewarded For What You Know," encouraging people to come forward to report suspected Medicare fraud.

Here are some common, real lawsuits happening to medical practices stemming from these internal enemies:

A California-based psychiatric medical services provider failed to provide a patient with timely access to the requested medical records and charged what the patient deemed as an "unreasonable fee" when the records were eventually provided. OCR also identified issues with the notice of privacy practices and a HIPAA privacy officer had not been appointed. The case was settled, and a financial penalty of $28,000 was paid. What's worse is now this is a first-time offense, so the penalties are light. If another case is proven, their fines will double or triple, and cases like this are growing in number. All it takes is someone in your office to get too busy and make an honest mistake of not providing medical records to a patient.

In another case, a dental practice owned by Dr. Phillip Igbinadolor, with offices in Charlotte and Monroe, NC, impermissibly disclosed a patient's PHI on a webpage in response to a negative online review. The failure to cooperate with the investigation and respond to an administrative subpoena resulted in a civil monetary penalty of $50,000. Again, this was an honest mistake taken by a well-meaning employee that now puts this small dental practice at more risk and higher fines.

A few years ago, there was a proposed rule that would dramatically increase the reward to Medicare Fraud Whistleblowers, from a current maximum of $1,000 to nearly $10 million. In addition to fueling the wrath of an already frustrated client or employee, these rewards provide a powerful incentive for plaintiffs and their attorneys to closely monitor covered entities and business associates for HIPAA violators.

It's not a stretch to imagine an unhappy patient, employee or ex-business associate lodging a HIPAA complaint against you or your organization as a way of getting revenge for what they feel is unfair treatment, jealousy or simply because you're "rich" and they're not.

Because they are the "enemy within," they are savvy enough to know (or at least suggest) that you have engaged in Willful Neglect because they know you have no policies and procedures, risk assessments, workforce training standards or documentation of HIPAA compliance. Their report triggers a mandatory HHS investigation where you could be slapped with a huge fine, not to mention the massive distraction it becomes for you and your staff. Of course, all of this could be avoided, or at least minimized, with some basic leg work before the complaint and minimal changes to procedure following it.

If You Won't Secure Your Data For You, Then At Least Consider Your Most At-Risk Patients

Recently I had a doctor running a non-compliant, non-secure small medical practice say to me, "HIPAA compliance is a joke. I'm not going to get audited or breached. Who's going to come and get me anyway…the HIPAA police? I'm not spending another dime on compliance or security."

Hopefully you aren't as arrogant as this particular doctor. However, you might not be taking this as seriously as you could. Maybe you don't care if you get audited or fined. Maybe you feel comfortable with your current security protocols and are willing to take the risks. But what about your patients? Do you believe they would have the same tolerance for risk when it comes to their private health information being exposed?

Your patients' medical records are *extremely* valuable to hackers. **The going rate on the Dark Web for a medical record is $1,200!** Hackers are running a business, and the people buying those records are going to use your patient's identity to purchase prescriptions and drugs, receive treatments or make fake medical claims to collect cash. They aren't paying $1,200 a record to use it to hack a Facebook account because there's no money in that. They are going to use it to buy things that create bills that are passed on to your patients to deal with.

That's because medical records tend to have more personal information in them than a breach on social media or from a credit card. Medical records have birthdays, social security numbers, credit card data and full contact information. In many cases, they have work information, such as their employer, job title, occupation, and salary.

We all know the elderly are most at risk for a scammer – and by allowing a breach to happen, you just handed sophisticated criminals the keys to take advantage of your most vulnerable patients.

As another doctor pointed out to us, they feel the Hippocratic Oath of "do no harm" extends beyond medicine and applies to all things a patient puts in your care. As a doctor, you know that prevention is the BEST medicine – and that's why you need to do everything in your power to prevent a cyber-attack that will expose your patients' medical records.

In A World Full Of Marketing Promises, How Do You Know Your Current IT Company Is ACTUALLY Doing A Great Job?

It's very possible that you are being ill-advised by your current IT company. What have they recently told you about the new threats emerging over the last 3-6 months? Are they meeting with you on a quarterly basis to go over a recent scan of your environment to ensure you are still secure? Situations can change in an instant – if they are not truly monitoring your environment

daily, scanning quarterly and in constant communication with you (or a key person on your staff) about security, they are NOT doing their job.

There could be several reasons for failing you.

First, and most common, they might not know HOW to advise you, or even that they should. Many IT companies know how to keep a computer network running **but are completely out of their league when it comes to dealing with the advanced cybersecurity threats we are facing today**. At a recent conference of my peers, I was shocked to learn many of them haven't even read the NIST framework and are unfamiliar with the actual HIPAA laws and guidelines. They're utterly clueless about compliance. That doesn't stop them from selling you IT services. They might even tell you that they're keeping you secure; but when you get breached, they'll point the finger at you saying YOU didn't want to spend the money on security, and they didn't warranty you wouldn't get breached or that they were keeping you compliant, leaving you to handle this on your own and carry the damages and cost.

Here's a test: E-mail them and ask them, point black, "Can you assure me you are doing everything we should to ensure we are HIPAA compliant and secure?" If they say yes, ask them to demonstrate it. You might find out that their story falls apart like a cheap suit. NOBODY (particularly IT guys) likes to admit they are out of their depth. They feel compelled to exaggerate their ability to avoid being fired and replaced – but it falls upon YOU to make sure you have the RIGHT company doing the RIGHT things.

Second, they may be "too busy" themselves or not have sufficient staff to truly be proactive with your account – which means they aren't doing the ongoing work that needs to be done (and they might still be charging you as if they were).

Third, they might just be cheap and unwilling to make significant investment in the tools, people and training they need. Maybe they don't want to admit the service package they sold you has become OUTDATED and inadequate. Their cheapness CAN be your demise.

Is Your Current IT Company Doing Their Job?
Take This Quiz To Find Out

If your current IT company does not score a "Yes" on every point, they are NOT adequately protecting you. Don't let them "convince" you otherwise and DO NOT give them a free pass on any one of these critical points. Remember, it's YOUR practice, income and reputation on the line.

That's why it's important to get verification on the items listed. Simply asking, "Do you have insurance to cover our practice if you make a mistake?" is a start, but getting a copy of the policy or other verification is critical. When push comes to shove, they can deny everything.

☐ **Have they met with you recently – in the last 3 months – to specifically review and discuss what they are doing NOW to protect you?** Have they told you about new and inexpensive tools such as 2-factor authentication or advanced endpoint security to protect you from attacks that antivirus is unable to detect and prevent? If you are outsourcing your IT support, they should, at a MINIMUM, provide you with a quarterly review and report of what they've done – and are doing – to protect you AND to discuss new threats and areas you will need to address.

☐ **Do they proactively monitor, patch and update your computer network's critical security settings daily? Weekly? At all? Are they reviewing your firewall's event logs for suspicious activity?** How do you know for sure? Are they providing ANY kind of verification to you or your team?

☐ **Have they ever asked to see your cyber liability insurance policy?** Have they verified they are doing everything your policy REQUIRES to avoid having a claim denied in the event of a cyber-attack? Insurance companies don't make money paying claims; if you are breached, there will be an investigation to prove you weren't negligent and that you were actually doing the things you've outlined on your policy.

☐ **Do THEY have adequate insurance to cover YOU if <u>they make a mistake</u> and your practice is compromised?** Do you have a copy of THEIR CURRENT policy? Does it specifically cover YOU for losses and damages? Does it name you as a client?

☐ **<u>Have you been fully and frankly briefed on what to do IF you get compromised</u>?** Have they provided you with a response plan? If not, WHY?

☐ Have they told you if they are outsourcing your support to a 3rd-party organization? **DO YOU KNOW WHO HAS ACCESS TO YOUR PRACTICE AND THE DATA IT HOLDS?** If they are outsourcing, have they shown you what security controls they have in place to ensure that a rogue technician, living in another country, would be prevented from using their free and full access to your network to do harm?

☐ **Have they kept their technicians trained on new cybersecurity threats and technologies, rather than just winging it?** Do they have at least ONE person on staff with CISSP (Certified Information Systems Security Professional) or CISM (Certified Information Security Manager) certification? Do they have anyone on staff experienced in conducting security risk assessments?

☐ **Do they have a ransomware-proof backup system in place?** One of the reasons the WannaCry virus was so devastating was because it was designed to find, corrupt and lock BACKUP files as well. <u>ASK THEM TO VERIFY THIS</u>. You might *think* you have it because that's what your IT vendor is telling you.

☐ **Do they have controls in place to force your employees to use strong passwords?** Do they require a PASSWORD management system to prevent employees from using weak

passwords? If an employee is fired or quits, do they have a process in place to make sure ALL passwords are changed? Can you see it?

☐ **Have they talked to you about replacing your old antivirus with advanced endpoint security?** Anti-virus tools from 2-3 years ago are useless against today's threats. If that's what they have protecting you, it's urgent you get it resolved ASAP.

☐ **Have they implemented "multifactor authentication" also called 2FA or "two factor authentication" for access to highly sensitive data?** Do you even know what that is? If not, you don't have it.

☐ **Have they recommended or conducted a comprehensive risk assessment every single year?** By law, you're required to do this, and your IT company should be handling the IT part of that for you.

☐ **Have they implemented web-filtering technology to prevent your employees from going to infected websites, or websites you DON'T want them accessing at work?** I know no one in YOUR office would do this, but why risk it? Adult content is still the #1 thing searched for online. Then there's gambling, shopping, social media and a host of other sites that are portals for hackers. Allowing your employees to use unprotected devices (phones, laptops, PCs) to access these sites is not only a security risk but a distraction where they are wasting time on YOUR payroll, with YOUR company-owned equipment.

☐ **Have they given you and your employees ANY kind of cybersecurity awareness training?** This is now required for HIPAA compliance and insurance companies to cover breaches. Employees accidentally clicking on a phishing e-mail or downloading an infected file or malicious application is still the #1 way cybercriminals hack into systems. Training your employees FREQUENTLY is one of the most important protections you can put in place. Seriously.

☐ **Have they properly configured your e-mail system to prevent the sending/receiving of confidential or protected data?** Properly configured e-mail systems can automatically prevent e-mails containing specified data, like social security numbers, credit cards, patient files and other sensitive data from being sent or received.

☐ **Do they allow your employees to connect remotely using GoToMyPC, LogMeIn or TeamViewer?** If they do, this is a sure sign to be concerned! Remote access should strictly be via a secure VPN (virtual private network).

☐ **Do they offer, or have they at least talked to you about, dark web/deep web ID monitoring?** There are new tools available that monitor cybercrime websites and data for YOUR specific credentials being sold or traded. Once detected, it notifies you immediately so you can change your password and be on high alert.

Security Is NOT Compliance –
Make Sure Your IT Company Is Taking These 3 Steps

As previously discussed in this report, a mistake many medical practices make is thinking because they're secure, they are automatically compliant. Not so. While security is definitely a part of compliance, there are 3 keys steps to ensuring you are actually compliant.

Most IT companies or HIPAA consultants are only doing 1 or 2 of the three. You want to make sure they are checking ALL the boxes so if and/or when a breach occurs and you get audited, you are brilliantly prepared, and the damages are minimized. Here they are in order:

1. A regular security risk analysis with a remediation plan.

You are legally required to conduct a risk assessment once a year. However, we recommend quarterly assessments to find security (and compliance) failings sooner so they can be addressed immediately. Doing assessments quarterly also allows you to break down the requirements for compliance and security into more manageable time frames (quarterly) instead of being hit with a giant project once a year. Problem is, this is where most small medical practices stop and don't go on to steps 2 and 3 below.

2. Full and true IMPLEMENTATION of the plan.

Best laid plans are worthless if not implemented. You can give a patient a treatment plan – but if they refuse to follow it, skip steps and cherry pick your advice, they cannot expect to get well.

Same goes with HIPAA compliance and security – your IT consultant should be giving you options, timelines and weighing the pros and cons of the choices you have about how to implement a plan to become compliant based on your risk tolerance, situation, budgets, resources, etc. A good IT company or consultant will guide you through this.

But the most important aspect is making absolutely certain that the IT team or company you put in charge to implement this plan is actually doing it. Based on our personal experience, 90% of the companies selling outsourced IT services and support are NOT being diligent about the full and complete implementation of a security and compliance plan.

In a world of marketing promises, how do you know your IT and security partner is delivering as promised? Please see the previous section of this report to know if they are truly implementing the plan. Further, we are offering a free, independent Risk Assessment to audit your current IT company and tell you the truth about what they are (or aren't) doing for you.

3. Documentation.

This is the part most IT companies and medical practices skip. Behind every security compliance measure is a documentation requirement. Practically every facet of HIPAA compliance requires that policies and procedures be created, implemented and documented. These documents must be retained for at least six years (state requirements may mandate longer retention periods).

If you have a breach and subsequently get audited, you will be required to produce the documentation of your security and compliance activities and policies.

Will You Wait Until You Actually Have A Breach Or A Report Filed Against You Before Doing Something About It?

Over half of all home security systems and cameras are bought (or beefed up) by homeowners *after* a burglary or home invasion. Across the country, warnings of bad storms drive hordes of people to the store to stock up on water, food and other supplies – and anyone who hesitates or waits to hit the store AFTER work or WHEN they have the time often arrives to find the store shelves empty, and the remaining picked-over supplies at jacked-up prices.

We are strongly cautioning against any assumption that you are truly protected and prepared should a breach occur, or you get reported for a violation. Fire prevention is infinitely cheaper, less stressful and more orderly than having to call the fire trucks and work the hose when your house is ablaze. Cancer is BEST treated when found EARLY and aggressively treated, not left to get worse until it reaches the point of no return.

The time to have an in-depth, fresh look at your HIPAA compliance is right now, with a trusted advisor who has your best interest in mind – NOT a government HHS auditor or an attorney – when there is no crisis happening, no auditors calling, no security breaches happening.

That's why we've set aside and reserved initial phone consultation appointment times with our most senior HIPAA and security leadership team members for the medical practices we serve as clients, as well as those who are not clients but are looking for a qualified third party to have "fresh eyes" on your current HIPAA policies and procedures to conduct a free, pre-emptive, independent risk assessment.

Our Free Preemptive IT Security Risk Assessment Will Reveal If Your Current IT Company Is Doing What They Should

Over the next couple of months, we will be conducting free Risk Assessments for medical practices and covered entities to find and expose vulnerabilities and failings in your security BEFORE a cyber event happens.

Fresh eyes see things – so the biggest value of our Assessment is getting us to sit on YOUR side of the table to and give you straight answers to whether or not your IT company or person is actually doing what they should be doing to minimize your chances of experiencing a breach and minimize the losses that can occur. **You get a "Sherlock Holmes" investigating on <u>your</u> behalf.**

<u>Here's How It Works</u>: We will conduct a thorough, CONFIDENTIAL investigation of your IT network, backups and security protocols through the lens of not only an IT company, but also from a HIPAA compliance standpoint of an insurance provider. Your time investment is minimal: one hour for the initial meeting and one hour in the second meeting to go over our Report of Findings.

When this Assessment is complete, here are just a few of the most frequently discovered problems that we are likely to uncover and answers we'll be able to provide to you.

- Is your current IT company or team **actually implementing critical security protections**, protocols and systems that would not only minimize the chances of a breach, but also ensure any insurance claims would not be denied for failing to follow through on something YOU agreed to do on your insurance policy's declarations contingent for coverage?

- Whether or not you would be able to say "Yes" to 20 simple questions any HHS auditor will ask you to determine if you're HIPAA compliant. These are painfully obvious questions you should be able to confidently say "yes" to. If not, your IT company (or whomever is advising you on HIPAA compliance and security) is failing you.

- What the least expensive, most impactful things you can do to secure your network and avoid getting slapped with "Willful Neglect" penalties should a breach happen.

- Are you able to pass a simple PEN test (penetration test)? We'll conduct one and be able to demonstrate, in a matter of hours, if your IT company is doing their job or completely failing you.

All of these are tiny "ticking bombs" in your security, waiting to go off at precisely the wrong time. We urge you to go to the URL below and book your free assessment now:

www.tech-adv.com/penetration-test/

TECH ADVISORS
IT Support and Cybersecurity Management

When *Others* Audit – Insurance Companies, Government Regulators – There Is No Kindness

Government auditors and insurance providers won't give you the benefit of the doubt. They know what to look for, where the failings typically occur. They are experienced in finding lax protocols and know what stones to turn over.

When such audits reveal problems, there is serious stress and strain placed on your staff, on your Practice Administrator and on you personally. Tensions rise, fingers get pointed and resentment can build. Your own preventive, independently conducted, completely confidential compliance assessment is the ONLY practical way to prevent embarrassment or other dire consequences. It's also the smart way to unearth problems you can fix now.

Candidly, no one should proofread their own work – so if you do have an IT company or HIPAA auditor you are paying, this will give you a free, no-risk way to tell for sure if they are doing the job you're paying them to do.

Please…Do NOT Just Shrug This Off (What To Do Now)

If you have scheduled an appointment, you don't have to do anything but be sure to show up, ready with any questions you might have.

If you prefer to talk to us first, call us at 508-356-5565 or send me an e-mail at konradm@tech-adv.com.

I know you are *extremely busy* and there is enormous temptation to discard this, shrug it off, worry about it "later" or dismiss it altogether. That is, undoubtedly, the easy choice…but the easy choice is rarely the RIGHT choice.

This I can guarantee: At some point, you will have to deal with a cyber security "event," be it an employee mistake, small breach or even a ransomware attack.

We want to make sure you are brilliantly prepared for it and experience only a minor inconvenience at most. But if you wait and do nothing and ignore our advice, I can practically guarantee it will be a far more costly, disruptive and devastating situation.

You've spent a lifetime working hard to get where you are today. Let us help you protect and preserve it.

Dedicated to serving you,

Konrad Martin

Web: www.tech-adv.com
E-mail: konradm@tech-adv.com
Phone: 508-356-5565

Here's What Our Clients Have To Say:

We Count On Tech Advisors

Working in the healthcare investment and consulting field, it's extremely important to be connected 24/7 and protected against cybersecurity threats. Tech Advisors ensures and manages the security at my office by upgrading our networks and services whenever necessary. Their goal has always been to protect our IT infrastructure and systems, so we can focus on our clients. I can always count on the Tech Advisors team take care of us.

Managing Director
Healthcare Capital

10 Years Greatly Appreciated

For over a decade, Tech Advisors has been our dedicated partner in ensuring all facets of our technology environment run smoothly. They understand that downtime is bad for business and so their responsiveness – weekdays, evenings, weekends – is fantastic and ensures we can provide uninterrupted service to our clients. Further, Kevin and Konrad are our strategic partners, keeping us up-to-date with emerging technologies and systems, implementing what makes sense for us and thereby enabling us to keep pace with our competitors. They and their staff are dedicated professionals who are great at what they do so that we can keep our focus on being great at what we do!

Managing Partner
Johnson O'Connor

Light Years Above the Competition

Their overall knowledge of IT and how they structure their systems, solutions, and price point, all are light years above what other IT providers have done for us…The way they build the technology, the way they architect it, the way they use the cloud – they have a much better sense and understand of how to put it all together… They've taken our technology to a whole other level. I could not afford to be down technologically as a company doing what we do: HR, payroll, and benefits. We have to be up all the time…But they monitor everything. And they are proactive. They come to us and say 'we need to do this, or we need to do that. They're phenomenal. I cannot say enough great things about their company.

CEO
HR Knowledge

Tech Advisors Client Since 2002

It is a tremendous opportunity for small businesses to have access to Tech Advisors' unique set of skills. Their combined knowledge of accounting and technical expertise proved invaluable to us at CAPCO. They were a pleasure to work with, and they offer the total package at a very competitive price. They really are ahead of the game.

President
CAPCO Energy Supply

Downtime no longer an Issue

Given that we're a New England business, we're frequently affected by weather, but I can't close up shop every time we're predicted for a Nor'Easter (which last winter would have meant the whole month of March!).

Last February our Wayland location lost power for three days. Because we keep our server in the cloud with Tech Advisors, our employees could work from home or in our Shrewsbury location. Everything ran smooth, and we were back to normal in Wayland as soon as the power returned, almost as if nothing happened.

Tech Advisors has given our company the ability to run smoothly no matter the weather – allowing our employees to work safely from home when necessary, while still providing them with opportunities for collaboration. They're ready for anything!

Partner
Paresky Flitt & Company, LLP

Please visit www.tech-adv.com/client-testimonials/ to view more of our client's testimonials.