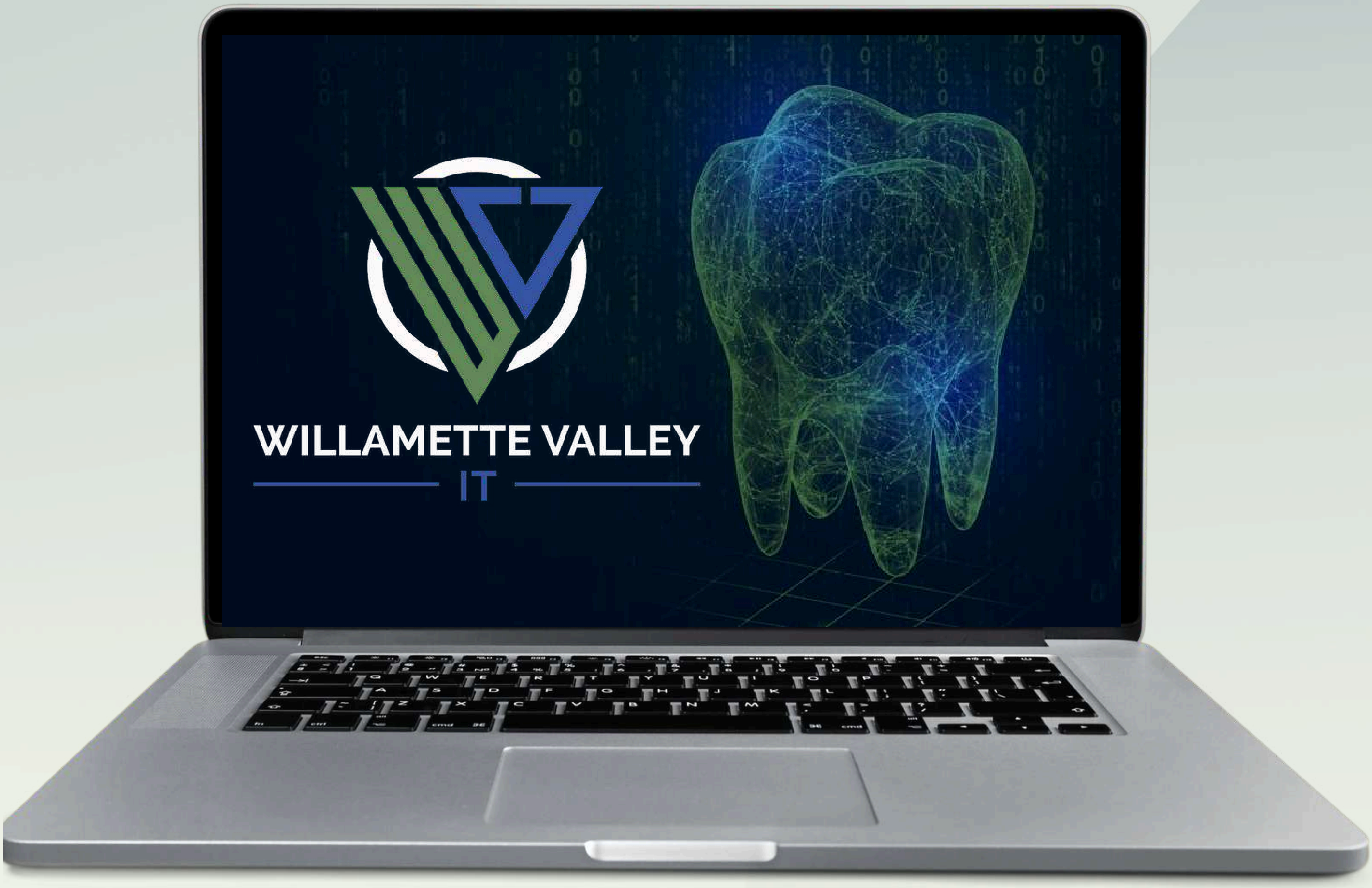
Protecting Your Patients, Your Practice, and Your Peace of Mind

A Dentist’s 2026 Guide to Cybersecurity, Data Protection, and Compliance Confidence



www.wvitpro.com

About The Author

Michael Amador

Owner/Tech/Cool Dude

Michael Amador is the founder of Willamette Valley IT, a Portland-based firm specializing in secure, compliant, and stress-free technology solutions for dental practices. A member of a multi-generational dental family, he combines deep industry insight with a consultative approach that helps dentists focus on patient care while he handles the tech.

WILLAMETTE VALLEY IT

www.wvitpro.com

What No One Tells Dentists About Cybersecurity Until It's Too Late

You've spent years building a trusted dental practice. The systems run, patients smile, and your team keeps things moving while your IT quietly holds it all together.

You probably assume your practice is protected, that your IT provider has safeguards in place, that you are close enough to compliant with HIPAA, and that your cyber insurance will step in if needed. You might even believe hackers only target large healthcare networks, not small local offices.

The truth is, those assumptions were once safe. They are not anymore. Cyberattacks on small healthcare practices have surged, and new rules for data security, insurance coverage, and compliance have changed the landscape. Even one small oversight can now lead to denied insurance claims, HIPAA violations, or devastating data loss.

If your cybersecurity plan has not been updated since before 2023, it is already out of date.

Even if you think you are covered, there is a good chance you are not. And when a breach occurs, your IT provider or insurer may not be the safety net you expect.

This guide is not meant to alarm you. It is designed to help you regain control, replace uncertainty with clarity, and follow a clear path toward lasting protection and peace of mind.

Because at the end of the day, cybersecurity isn't about firewalls and jargon. It's about protecting the trust your patients place in you, every single day.

The goal is to protect you from ever being caught off guard by a cyber incident and thinking, "If only someone had told me what to watch for."

This isn't just about checking the HIPAA or PCI compliance boxes. It's about truly understanding the risks that come with a cyberattack, an IT failure, or even a simple employee mistake. When those events happen, the costs, the stress, and the damage to your reputation can be staggering.

That's why this guide exists. Over the past few years, our team has assessed dozens of dental and medical practices before they became clients. Not one of them was fully prepared for a security incident. None could have passed a complete compliance audit without help.

Every one of them believed they were secure enough. Every one of them underestimated the financial and emotional impact of a data breach. And in nearly every case, their so-called experts, their IT provider, their software vendor, or even their insurance rep, had failed to prepare them for what could really happen.

If that sounds familiar, you are not alone.

The reality is that if your practice were hit with a cyber incident tomorrow, your staff would suddenly be dealing with chaos. You would have investigators, auditors, and attorneys demanding immediate information. You would face emergency IT costs, legal fees, and government fines. You would have to fight to restore your systems while trying to keep your patients' trust intact.

And here’s something most people never realize until it’s too late: insurance companies can deny cyber claims if certain protections weren’t in place before the breach. In other words, if your safeguards don’t meet updated standards, your coverage might not apply at all.

This isn’t something you can afford to delegate entirely to an administrator or assume your IT company has handled. Just because your practice management software is “HIPAA compliant” doesn’t automatically mean your entire network is. As the practice owner, you are ultimately responsible for how patient data is protected and for any loss that occurs.

Small dental and medical practices are now the number one target for cybercriminals. They are attractive because they hold valuable data but often lack the same security resources as hospitals or large healthcare systems. The truth is, most practices have not been given a plan that is complete, practical, and affordable. Think of it this way: your cybersecurity plan might look fine at first glance, but if it has gaps, it’s like a parachute with holes in it. You only realize the problem when it’s too late to fix it.

This guide will help you patch those holes and give you a clear, confident path forward.

If your IT company or CIO has not recently talked with you about emerging security threats and what they mean for your practice, now is the time to close that gap. Read this guide carefully and take proactive steps to strengthen your protection.

“A Breach Won’t Happen To Us. We’re Too Small, Too Smart, and Too Careful.”

It’s easy to believe that your practice is safe. You might think hackers only go after hospitals, large healthcare networks, or national brands. You might trust that your staff would never fall for a phishing email or that your systems are too simple to attract attention.

That sense of comfort is exactly what cybercriminals rely on.

Smaller healthcare practices are often the easiest to compromise. Hackers know you have valuable information such as patient records, credit card data, and personal details, but you may not have the same level of protection as larger organizations. You are not invisible to them. You are often seen as an easy doorway.

Most of the time, these attacks are not personal. Cybercriminals use automated software that scans the internet around the clock, looking for any weak system or outdated software to exploit. When they find one, they strike.

It is not about who you are. It is about how easy you are to access.

Studies show that small and mid-sized healthcare practices experience multiple attempted cyberattacks every year. You rarely hear about them because they are quietly resolved or kept private to avoid negative publicity. But the consequences are real.

Even more concerning, most small businesses are not financially ready to recover from a cyber incident. Many cyber insurance policies are now stricter, and claims can be denied if required protections were not in place before the attack.

Many practice owners believe their IT company has handled everything, only to discover later that essential safeguards were missing.

The result can be overwhelming. Data loss, denied claims, public trust shaken, and long nights wondering how to recover.

You may not see these stories on the evening news, but they happen every single day to businesses that look just like yours.

This guide is not here to frighten you. It is here to bring clarity. When you understand how these attacks happen and what steps truly protect your data, you can move forward with confidence and peace of mind.

The Real Cost of “It Won’t Happen To Us”

If a data breach occurs, regulators will not ask whether you meant to protect patient information. They will ask what steps you actually took. As a healthcare provider, you carry a legal responsibility to secure patient and client data. Failing to do so can result in serious financial and professional consequences.

Saying “I didn’t know” will not hold up in court or with government agencies. Cyber incidents have been a known risk for years, and regulators expect every healthcare organization to take reasonable, documented precautions.

It is worth asking yourself a few hard questions. Are you completely certain that your practice is too small for hackers to notice? Are you sure you could absorb the cost of a ransomware payment, legal defense, and the loss of patient trust if your data were exposed?

The numbers tell a sobering story. ***The average ransomware demand now ranges between $2,000,000 and $5,000,000, and that figure continues to climb***. That amount does not include legal penalties, emergency IT recovery work, or the revenue lost while systems are offline.

Category	Average Cost or Fine
Average Ransomware Recovery Cost	$100,000
HIPPA Fine per Wilful Violations	$50,000
HIPPA Fines - Repeated Violations	Up to $250,000
PCI Compliance Fines	$5,000 - $100,000 per month

A single ransomware event can cause both immediate losses and long-term penalties. Prevention is always more affordable than repair.

These numbers are not hypothetical. They come from real cases affecting healthcare providers nationwide.

Large organizations often recover because they have full teams for compliance, cybersecurity, and legal response. Small dental practices do not have that safety net, which makes proactive planning essential.

A breach costs more than money. It can damage your reputation, your staff morale, and your patients' trust. Prevention is always simpler and less costly than repair.

This guide will show you how to stay compliant, stay protected, and keep your focus where it belongs: on your patients.

Take the First Step Toward a Safer, More Confident Practice by Scheduling Your Complimentary Cybersecurity and Compliance Assessment
Call our office at (503) 856-6897.

How Bad Can It Be? My Insurance Will Cover Me, Right?

It is natural to assume that your insurance will protect you if something goes wrong. After all, that is what insurance is for. Unfortunately, cyber insurance does not always work the way most practice owners expect.

Insurance companies exist to make money, not to pay claims. Only a few years ago, most carriers kept about 70% of their premiums as profit and paid out 30% in claims. That balance has now flipped. The number of cyber incidents has skyrocketed, forcing insurance companies to tighten requirements and reduce payouts.

Today, even getting approved for a basic cyber liability policy can be difficult. Carriers often require proof that your practice has specific safeguards in place. These can include multifactor authentication, password management systems, anti-phishing protection, employee cybersecurity training, and secure offsite backups.

Some carriers now go further, asking for written documentation such as a formal cybersecurity policy, a Business Continuity Plan, or a Written Information Security Plan (WISP). Each insurer has its own checklist, and the requirements become stricter every year.

The greatest risk for most small healthcare practices, however, is not just getting coverage. It is keeping it valid.

When a breach occurs, insurance carriers do not automatically issue payment. They launch an investigation. They look closely at whether the required security measures were actually implemented and maintained. If even one critical step was skipped, the claim can be denied.

In some cases, the insurer may argue that the business refused recommended upgrades or declined advanced protections that were offered. Without documentation that shows your practice followed cybersecurity best practices and took reasonable precautions, the burden of the incident can fall entirely on you.

That means paying for recovery services, legal fees, and lost revenue out of pocket.

Your cyber insurance policy is only as strong as the proof that you have done your part to protect patient and client data. This guide will help you understand what insurers look for and how to build the kind of documentation and protocols that actually hold up under review.

Exactly How Can Your Business Be Damaged By Cybercrime And A Known Data Breach Of Sensitive Data?

1. Loss of Patients and Revenue

When a breach happens, you are required to notify your patients that their personal or financial information may have been exposed. Some patients will understand and stay with you. Others will lose confidence and move on.
In today's world, news spreads fast. A single post on social media can reach hundreds of people in minutes. Even if only a small percentage of your patients decide to leave, that loss can quickly snowball. ***Losing twenty percent of your patients can easily mean losing years of hard-earned trust and future referrals***.

Once confidence is shaken, it is very hard to rebuild. Patients want to know that their health information is safe and that their dental provider takes security seriously.

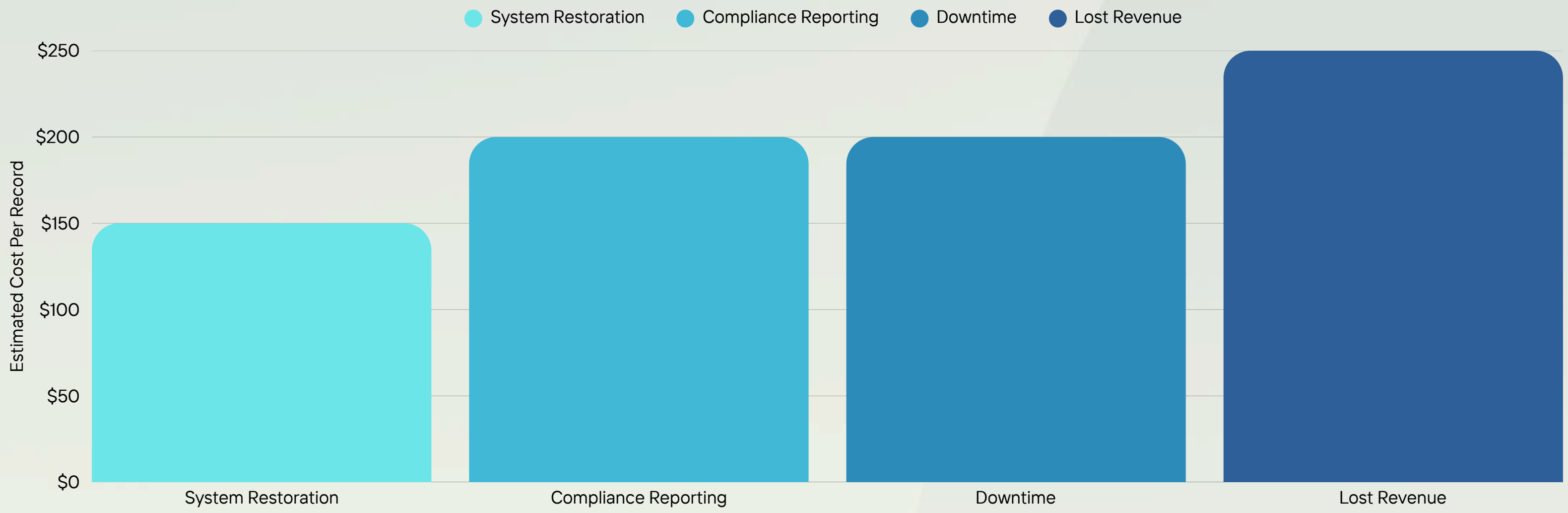
2. Legal Fees, Compliance Fines, and Lawsuits

If a data breach occurs, timely support from an experienced IT partner helps you recover quickly and keep your practice running smoothly. You may also need to hire legal counsel to help navigate investigations and compliance requirements.

Even if you avoid direct fines, you will spend valuable time gathering records, answering auditor questions, and demonstrating compliance. For small practices, that can mean pulling staff away from patient care for days or even weeks.

Government regulators and insurance auditors will expect full transparency. You will be asked to show exactly how your systems were secured, how the breach occurred, and what steps you took to prevent it. This process can be expensive and emotionally exhausting.

3. Ongoing Costs and Operational Disruption



(Average total cost per lost or stolen record: $150-$250)

** Multiply that by the number of patient records your practice stores to see how quickly the costs add up.*

For healthcare organizations, the costs climb even higher. The State of Ransomware in Healthcare report by Sophos* revealed that ***60% of healthcare organizations that suffered data encryption ended up paying the ransom***.

Beyond that, you may also face these additional expenses:

- Credit and identity theft monitoring for each affected patient, typically $10-$30 per record.
- Notification costs for printing and mailing letters to patients, which are legally required in most states.
- Staff time spent managing communications, handling questions, and completing additional documentation for auditors.
- IT remediation work and vendor coordination to ensure every compromised system is secured and verified.
- If your practice processes credit card payments, you may face PCI compliance fines ranging from $5,000 to $100,000 per month until issues are resolved.
- Higher credit card processing fees or even temporary suspension of your merchant account.

The total financial impact can quickly reach hundreds of thousands of dollars, but the emotional toll is often greater. You built your practice on trust and care. A cyber incident can shake both.

The purpose of this guide is to help you understand these risks so you can prevent them. With the right protections, training, and response plan, you can safeguard your patients, your staff, and the reputation you have worked so hard to build.

**The state of Ransomware in healthcare 2025 report. SOPHOS. (n.d.). https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-healthcare*

The Real Risk Often Comes from Inside the Practice

Many practice owners worry about government audits, but the truth is that most compliance investigations do not begin with an official inspection. They start with a complaint.

Those complaints usually come from two places. The first is an actual cyber incident, such as a ransomware attack or data breach. The second, and often more surprising, is from inside the organization.

A compliance investigation can be triggered by a frustrated employee, an unhappy former team member, or even a patient who feels mistreated. Sometimes the complaint is based on a misunderstanding. Other times, it is made out of frustration or anger. Either way, it can create major disruption for your practice.

There are law firms that actively advertise online for whistleblower cases. They encourage individuals to report potential HIPAA, PCI, or data privacy violations and may even offer financial incentives to do so. These programs are protected by law, and anyone who files a report may be shielded from retaliation.

For a dental practice, the most common risk is not intentional wrongdoing. It is the appearance of neglect. If a current or former employee knows that your team has not completed formal security training, performed a risk assessment, or documented compliance policies, that can be enough to raise concern.

Once a complaint is filed, a formal investigation begins. Regulators will request documentation and evidence of compliance efforts. If that information does not exist, the process can lead to steep fines and significant stress for everyone involved.

The good news is that this kind of situation is preventable. By putting clear policies in place, conducting regular staff training, and maintaining up-to-date documentation, you can dramatically reduce both the likelihood and the impact of any complaint.

Preparation is always easier and less costly than reaction. A few simple steps today can save countless hours and expenses later. This guide will help you understand what those steps are and how to implement them without disrupting your day-to-day work.

If You Will Not Secure Your Data for Yourself, Do It for Your Patients

Not long ago, a doctor running a small medical office said something that stayed with me. He told me that HIPAA compliance was unnecessary and that he was not worried about getting audited or hacked. He laughed and said, “Who is going to come after me anyway? The HIPAA police?”

If you knew your own doctor felt that way about your medical records, how would that make you feel?

Most dental professionals care deeply about their patients and would never take that kind of risk intentionally. Still, many practices underestimate the seriousness of compliance and assume their systems are secure enough. Others believe the risk of a breach is too small to justify the investment in stronger protection.

But this is not only about your comfort level with risk. It is about your patients and the trust they place in you every single day.

When patients share personal information with your practice, they are giving you more than just a name and a date of birth. You may have access to their medical history, financial data, insurance details, and even Social Security numbers. All of that information can be sold or misused by criminals in ways that cause lasting harm.

Stolen data can be used to file false tax returns, take out loans, or even purchase prescription drugs under someone else's identity. In some cases, patients only learn about the problem when they receive unfamiliar bills or collection notices.

Protecting that information is an extension of the same ethical promise every healthcare provider makes: to do no harm. In the modern world, that promise includes keeping patient data safe.

Prevention is the best medicine. Strong cybersecurity, regular staff training, and a proactive compliance plan protect not only your practice but also the people who trust you with their most private information.

Your patients rely on you for care. They also rely on you for confidentiality.

How to Know if Your Current IT Provider Is Truly Protecting You

In a world full of promises and polished marketing, it can be difficult to know whether your current IT provider is actually doing a great job.

Ask yourself a few simple questions. When was the last time your provider updated you on new cybersecurity threats? Have they met with you in the past quarter to review a security scan or discuss new risks? Are they monitoring your systems every day and sharing reports about your protection status?

Technology changes quickly, and so do the tactics of cybercriminals. If your provider is not checking in regularly, running quarterly scans, or staying in active communication with you or your office manager, they may not be keeping your practice as safe as you assume.

There are several possible reasons for this gap. The most common is that many IT companies simply do not specialize in healthcare or dental environments. They may know how to keep a network running and how to troubleshoot software problems, but cybersecurity for healthcare requires far more expertise.

Protecting patient data, maintaining HIPAA compliance, and managing secure backups all require deep knowledge of how dental systems, imaging software, and patient databases interact. Many general IT companies lack that level of specialization.

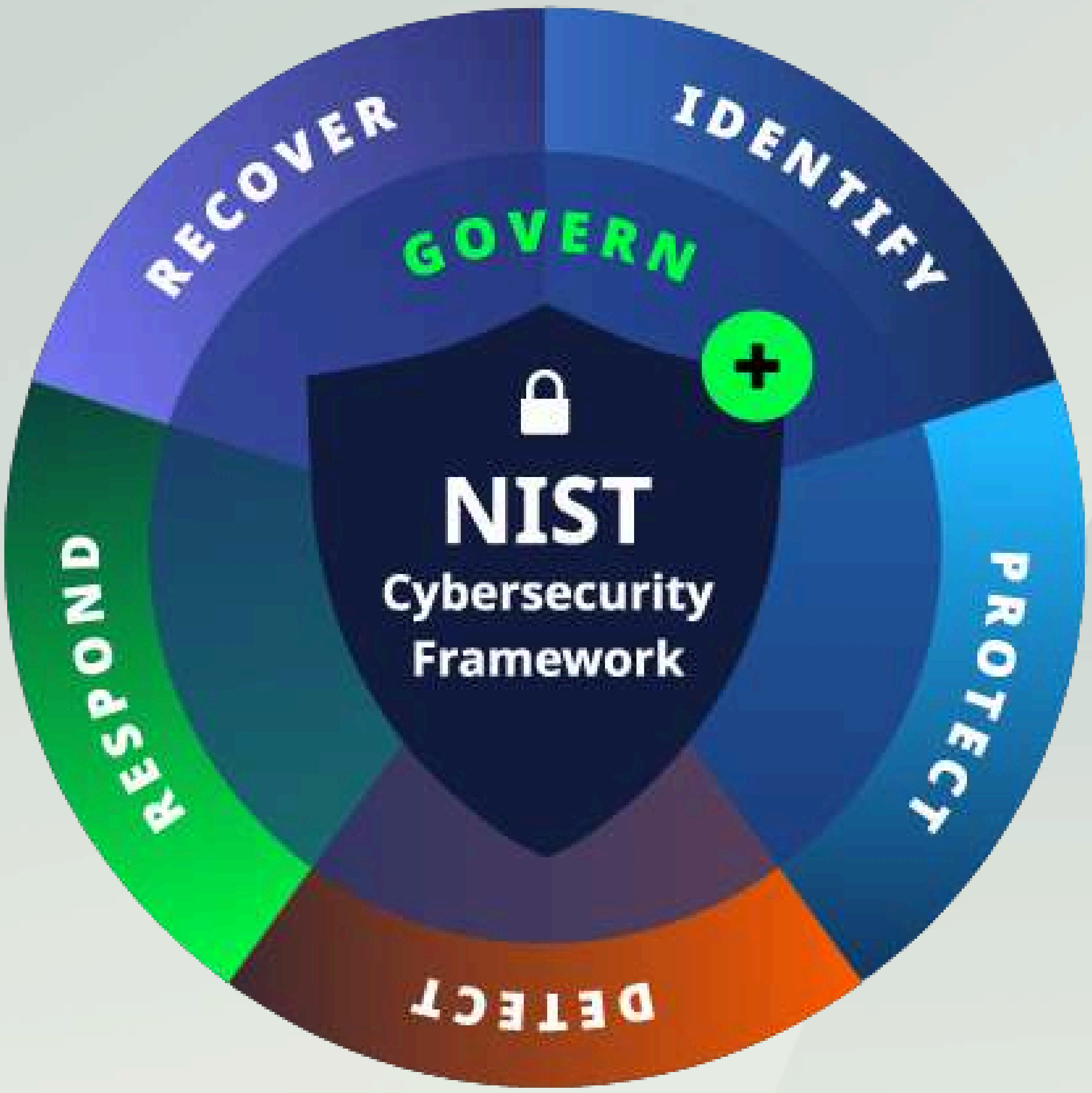
You deserve a partner who treats your data with the same care you give your patients. A trusted IT team should be proactive, transparent, and focused on prevention rather than reaction.

If your current provider is not helping you stay ahead of emerging threats, it may be time to ask harder questions about what they are truly doing to protect your practice.

It can be difficult to know whether your current IT provider is truly keeping your practice secure. Ask yourself when they last updated you on new threats, reviewed a recent security scan, or met with you to discuss your protection plan. If that has not happened recently, your practice may not be as safe as you think.

Many IT providers are skilled at keeping networks running but lack real experience with healthcare compliance. Protecting patient data and maintaining HIPAA standards requires specialized knowledge that general IT companies often do not have.

At a recent industry conference, many providers admitted they had never reviewed the NIST cybersecurity framework or studied HIPAA, PCI, or GLBA requirements. Despite this, they continue to sell IT services to healthcare practices. When breaches occur, they often shift responsibility back to the client, leaving the practice owner to handle the fallout.



NIST's Cybersecurity Framework, developed by the National Institute of Standards and Technology, outlines five core functions: Identify, Protect, Detect, Respond, and Recover. It helps organizations manage and reduce cybersecurity risks with a clear and structured approach.

When you start asking questions, you might notice that their explanations do not add up. Some IT providers exaggerate their expertise to avoid admitting they are out of their depth. Others are simply too busy to give your account the proactive attention it needs.

Here's a quick test for your I.T. person or company. E-mail them and ask them, point blank, "Can you assure me you are doing everything we should to ensure we are compliant and secure from a data breach?" If they say yes, ask them to demonstrate it.

There are also those who cut corners, using outdated tools or avoiding necessary investments in staff training. They may still charge as if they are providing premium service, even when they are not keeping pace with modern security standards.

The bottom line is that it is your responsibility to ensure you have the right company doing the right work. A trustworthy IT partner will be transparent, accountable, and proactive in protecting your practice. Anything less puts your patients, your data, and your reputation at risk.

Is Your Current IT Provider Truly Protecting You?

There are a few key things every IT company should be doing to keep your practice secure. If your current provider cannot answer “yes” to each of these questions, you may not be fully protected.

□ **Have they met with you recently to review your security and compliance?**
Your IT provider should meet with you every few months to review risks, share updates, and explain how they are protecting your practice. They should also provide reports and recommend affordable tools like multifactor authentication or cloud detection and response.

□ **Are they proactively monitoring and maintaining your systems?**
A reliable partner prevents problems before they start. Continuous monitoring, updates, and maintenance should be standard for every healthcare practice.

□ **Do you have a secure, immutable backup?**
A true backup cannot be altered or deleted, even by ransomware. Ask your provider to confirm that all server, cloud, and device data are protected and recoverable.

□ **Do you and your staff receive cybersecurity awareness training?**
Human error causes most breaches. Regular awareness training keeps your team alert and is now required by many insurance carriers and compliance standards.

□ **Have they reviewed your cyber insurance policy?**
Your provider should know your policy requirements and ensure your systems meet them. If protections are missing, your claim could be denied.

WILLAMETTE VALLEY
IT

www.wvitpro.com

Your IT provider should be more than a technician who responds to issues. They should be a partner who understands the business, legal, and ethical responsibilities that come with handling patient data. If they are not helping you stay ahead of these five critical areas, it may be time to find someone who will.

Additional Questions to Ask Your IT Provider

1. Do they have adequate insurance coverage?
Ask for a copy of your provider's current policy and confirm that it covers you as a client. Their insurance should protect you if they make a mistake that compromises your data or systems.

2. Have they given you a clear incident response plan?
You should know exactly what to do if your systems are compromised. If your provider has not provided a written plan or reviewed one with you, that is a serious gap in your readiness.

3. Are they outsourcing your support?
Find out whether any part of your IT support is handled by a third party. If so, ask who those providers are and what security controls prevent unauthorized access to your network and data.

4. Are their technicians properly trained and certified?
Cybersecurity changes quickly, and your provider's team should stay current. Ask if they have certified professionals such as CISSP or CISM specialists, or staff trained to conduct formal security risk assessments.

5. Do they enforce strong password management?
Your IT provider should have systems that require secure passwords, prevent weak ones, and automatically reset access when an employee leaves. These controls protect you from both mistakes and misuse.

6. Have they upgraded your antivirus to modern endpoint protection?

Antivirus tools from even a few years ago cannot stop today's threats. Your systems should be protected with current endpoint security that detects and isolates suspicious activity.

7. Have they implemented multifactor authentication?

Multifactor authentication, sometimes called two-factor authentication, is a basic yet critical defense. It protects your cloud apps, email, and patient systems from unauthorized access.

8. Do they perform a complete risk assessment each year?

Annual risk assessments are often required by law and are an essential part of your compliance strategy. Your provider should manage the IT portion and share the results with you.

9. Have they added web filtering for safe internet use?

Web filtering tools block access to dangerous or inappropriate sites that can introduce malware. This reduces both security risks and workplace distractions.

10. Do they control remote access securely?

Remote connections should always occur through a secure virtual private network (VPN). If your staff uses open tools like GoToMyPC or TeamViewer, your provider needs to replace those with secure alternatives immediately.

11. Is your email system properly configured for data protection?

A well-configured email system can automatically block messages that contain protected information such as Social Security numbers, credit card data, or patient records.

12. Do they monitor the dark web for stolen credentials?

Modern cybersecurity tools can scan dark web marketplaces for your email addresses or passwords. If stolen credentials are detected, you can act quickly to change passwords and protect your accounts.

13. Do they protect your cloud platforms with advanced detection tools?

Applications like Office 365 and Google Workspace are prime targets for attackers. Ask your provider whether they use cloud detection and response systems to monitor for suspicious activity.

If your IT provider cannot confidently answer "yes" to every one of these questions, it may be time to reevaluate your partnership. The right team will not only meet these standards but will also help you understand exactly how each layer of protection keeps your practice safe.

Will You Wait for a Breach Before Taking Action?

Most people buy home security systems only after a break-in. The same pattern holds true with cybersecurity. Many practices only invest in serious protection after they have already experienced an attack or compliance violation.

The problem is that waiting until after an incident is always more expensive and more stressful. ***Once a breach occurs, you are no longer making calm, informed decisions***. You are reacting under pressure, trying to limit the damage while regulators, attorneys, and insurers start asking difficult questions.

Prevention is always the smarter choice. Fire prevention is far easier and less costly than fighting a fire. Regular health checkups are more effective than waiting until a problem becomes severe. The same principle applies to cybersecurity. The earlier you identify and address weaknesses, the easier they are to fix.

Now is the time to take a fresh, honest look at your IT systems and data protection strategy. ***The best time to strengthen your defenses is when there is no crisis, no audit, and no breach to manage***.

Our team offers complimentary consultations for practice owners who want an independent, expert perspective on their current security and compliance readiness. During this session, we will review your systems, identify potential risks, and recommend practical next steps to strengthen your protection.

You do not have to face these challenges alone. With the right partner and a proactive plan, you can protect your patients, your reputation, and your peace of mind long before a crisis ever begins.

Your Complimentary IT Security and Risk Assessment

We offer complimentary IT and cybersecurity risk assessments for dental and medical practices throughout the region. This review is designed to uncover weaknesses and gaps in your security before a breach occurs, giving you the opportunity to address them while it is still easy and affordable to do so.

The goal is simple: to give you a clear, honest picture of how secure your systems really are and how well your current IT provider is protecting you. Think of it as having a fresh set of expert eyes reviewing your digital safety from your side of the table.

Our team approaches each assessment as a partnership. We take the time to understand your systems, your workflow, and your goals so that our recommendations make sense for the way your practice actually operates.

Your patients trust you. You can trust us to protect your technology. Call (503) 856-6897 to schedule your complimentary cybersecurity and compliance assessment.

Here is what to expect:
We begin with a short, confidential consultation to understand your current setup and concerns. After that, our cybersecurity team performs a detailed review of your network, backups, and security protocols. Your total time investment is about one hour for the first meeting and one hour for a follow-up to review our findings.

WILLAMETTE VALLEY IT

www.wvitpro.com

When your assessment is complete, you will receive a clear, easy-to-understand report showing:

- ✓ **Whether your systems and data are fully protected from hackers and ransomware, or where you may be exposed.**
- ✓ **Whether your data backups are complete, secure, and capable of fast recovery during an emergency.**
- ✓ **Where your practice may be at risk of noncompliance with HIPAA or other regulations.**
- ✓ **Opportunities to reduce IT costs while improving communication, performance, and staff productivity.**

Each finding is a chance to strengthen your practice and prevent small issues from becoming major problems.

Schedule your complimentary assessment today to take the first step toward greater security and peace of mind.

Click the link or contact our team to schedule your appointment.

WILLAMETTE VALLEY
IT

www.wvitpro.com

Why a Little Preparation Can Save a Lot of Stress

When insurance companies or government regulators audit a practice, kindness is not part of the process. Auditors know exactly what to look for. They understand where most practices fall short, and they are trained to uncover every weak point in your systems and procedures.

When problems are found, the stress can spread quickly. Staff members feel pressure, administrators scramble, and blame often follows. The best way to avoid that situation is to identify issues before anyone else does. ***A private, independent, and confidential compliance assessment allows you to find and fix problems quietly and on your own terms***.

No one should proofread their own work, and the same applies to cybersecurity. Even if you already have an IT provider or compliance consultant, an independent review gives you a clear and unbiased picture of how well they are protecting your practice. It is a smart, low-risk way to confirm that you are getting the service you are paying for.

What to Do Next

If you have already scheduled your complimentary assessment, simply plan to attend your appointment with any questions you want answered.

If you prefer to speak with someone first, you can reach our team by phone at **(503) 856-6897** or by email at **info@wvitpro.com**.

We understand how busy you are and how easy it is to set this aside for later. But waiting rarely makes things easier. Taking a small step now can prevent a far larger problem down the road.

Every dental practice will eventually face some kind of cybersecurity challenge, whether it is a phishing email, an employee mistake, or a ransomware attempt. The difference between disruption and disaster is preparation.

Our goal is simple: to make sure you are fully prepared, so that any incident becomes a small, manageable inconvenience rather than a crisis.

You have worked hard to build your practice and protect your reputation. Let us help you safeguard both.

Dedicated to your peace of mind,

Michael Amador

Michael Amador
Willamette Valley IT
Owner/Tech/Cool Dude
info@wvitpro.com
Phone: (503) 856-6897

WILLAMETTE VALLEY IT

www.wvitpro.com

What Portland Dentists Are Saying

Real stories from practices who trust Willamette Valley IT to keep their technology secure and stress-free

"The absolute best in the business. If you don't want an IT headache use these guys. If you want prompt service and great communication use these guys. If you want people that know any and all dental software, use these guys. These guys will make your workflow seamless. Mike and Gosta are knowledgeable and will treat you like family."

Justin Maristica, DMD
TenderCare Dental

"I have worked with WVIT for many years. They are always attentive and effective and keeping our IT working and they help us with the innovative video sharing and teaching needs that we have. I highly recommend WVIT for those who want a top-notch team of knowledgable IT professionals."

Kelly Blodgett, DMD, NMD, IBDM
Blodgett Dental Care

"We have been clients of Willamette Valley IT since day one! They are always helpful and prompt at acting on any problems/questions that may arise."

Dale Nelson, DMD
Salmon Creek Family Dental

WILLAMETTE VALLEY
IT

www.wvitpro.com