FOR PHYSICIANS, MEDICAL DOCTORS & PRACTICE OWNERS IN SOUTH FLORIDA

You became a doctor to treat patients.

Not to manage technology.

The plain-English guide for **South Florida physicians and practice owners** — what your IT company should be doing for your practice, what HIPAA requires of you personally, and the questions every doctor should ask before signing with an IT firm.

CONTENTS

What's inside.

FROM THE DESK OF HEBER RODRIGUEZ, PRESIDENT

You trained for years to treat patients.
Not to manage technology.

If you're a physician or practice owner in South Florida — and you're tired of technology problems eating into your patient time, creating HIPAA anxiety you can't get a straight answer on, or leaving you personally liable for decisions you didn't know you were making — this guide is for you.

I'm Heber Rodriguez, President of RRG Networks Solutions. We've served South Florida businesses and medical practices for over 10 years with a 97% client retention rate. Healthcare is one of the most demanding IT environments we work in — and also the one where bad IT causes the most harm. **When the EHR goes down, patients sit in the waiting room. When ransomware hits, you can't see charts. When a HIPAA breach happens, the 60-day clock starts the moment you find out.**

I wrote this guide because most IT companies talk over the people who actually own the risk. They use technical language with the one person in the building who carries the most personal liability — the physician. **As a covered entity under HIPAA, you are personally accountable.** Not your IT firm. Not your EHR vendor. You. That's why this guide is written entirely in plain English.

This guide is written entirely in plain English. No acronyms without explanations. No technical jargon. Just honest answers to the questions South Florida medical practices ask us every week — what HIPAA actually requires, what happens when your EHR goes down, how ransomware gets into a practice like yours, and what good IT support for a medical office actually looks like.

My goal is simple: give you the information you need to make the right decision — so you spend your days treating patients, not managing a technology crisis.

Heber Rodriguez
PRESIDENT · RRG NETWORKS SOLUTIONS

SOUTH FLORIDA'S HEALTHCARE IT SPECIALIST

The team behind 10+ years & 97% retention.

HIPAA-compliant by default. A signed BAA with every engagement. Built so that physicians can focus entirely on patient care — not on whether the EHR is running, whether patient data is protected, or whether the practice will pass its next compliance review.

RRG Networks Solutions serves South Florida medical practices, clinics, and behavioral health groups across Miami-Dade, Broward, Palm Beach, Collier, Lee, and Monroe counties — including Miami, Coral Gables, Aventura, Pembroke Pines, Doral, and Fort Lauderdale.

Our team includes full-time engineers and network specialists, supported by a 24/7 Security Operations Center for real-time threat monitoring. We sign a **Business Associate Agreement (BAA)** with every client — which means we're legally accountable as a HIPAA business associate, not just a vendor who says they're compliant.

Every engagement includes: a signed BAA, HIPAA risk assessment support, EHR uptime monitoring, endpoint security on every workstation, and a written incident-response plan. We scope to the size of your practice — a 2-doctor primary care office and a 15-provider specialty group have different needs and different budgets.

BY THE NUMBERS

What 10+ years looks like.

10+	**YEARS IN BUSINESS** Serving South Florida since 2016.
97%	**CLIENT RETENTION** Year over year. We earn it monthly.
24/7	**SECURITY OPS CENTER** Real-time threat monitoring.
BAA	**EVERY ENGAGEMENT** We sign a Business Associate Agreement with every client.

Compliance: HIPAA Privacy · HIPAA Security · HIPAA Breach Notification · HITECH · 42 CFR Part 2 · DEA EP

EVERY KIND OF MEDICAL PRACTICE IN SOUTH FLORIDA

Built for your type of practice.

A solo primary care doctor, a 10-provider cardiology group, and a behavioral health group each have different compliance obligations, different software, and different risks. We've worked in all three.

PRIMARY CARE & SMALL PRACTICE

1–3 Providers

HIPAA compliance, EHR uptime, and IT support that works without requiring you to manage it. Physicians in small practices often end up handling IT problems personally — between patients, after hours, or on weekends. That should never be your job.

Your biggest concern as a physician: Personal HIPAA liability from a breach you didn't cause — and an EHR outage that forces you to stop seeing patients with no one to call.

SPECIALTY & MULTI-PROVIDER

Cardiology, Ortho, OB/GYN & More

Multi-location ready. Multiple providers mean more accounts, more devices, more off-boarding when someone leaves, and more surfaces for a breach. We manage identity, devices, and PHI across all of it — without asking your front desk to become IT staff.

Your biggest concern: A new provider starting Monday with nothing provisioned, or a departed doctor whose login still works six months later.

BEHAVIORAL HEALTH & THERAPY

The Strictest Privacy Standard

Substance-use-disorder records (42 CFR Part 2) are subject to tighter rules than regular HIPAA. Even stricter access controls, tighter audit trails, and zero compromise on patient confidentiality. We understand the difference — most IT firms don't.

Your biggest concern: A records disclosure — even accidental — that violates 42 CFR Part 2 and carries federal penalties separate from HIPAA.

BOTTOM LINE

Whatever your practice type, the foundation is the same: HIPAA compliance, EHR uptime, and patient data that never ends up in the wrong hands.

SOUND FAMILIAR?

If any of these sound like your week, you're not alone.

6 SITUATIONS EVERY PHYSICIAN IN SOUTH FLORIDA RECOGNIZES

01	02	03	04	05	06
EHR Down at 8 a.m.	**Ransomware Note Found**	**Wrong Patient Data in Portal**	**Cyber Insurance Renewal Arrived**	**Doctor Left In March**	**New Provider Starts Monday**
12 patients arriving at 8:30	Every chart encrypted. $40K demand.	60 days to decide if you owe HHS a breach notice	12 new requirements you may not currently meet	Their login still works. Nobody turned it off.	EHR, email, billing, MFA — nothing is provisioned

→ *Friday 4 p.m. The EHR is down. Twelve patients in the waiting room, no charts, no schedules, and nobody on the phone with a real answer about when it comes back.*

→ *An email looks like it's from your insurance verification service. Someone on staff clicks it. Three days later: ransomware note, forty-thousand-dollar demand, every chart encrypted — and you're the one HHS calls.*

→ *A patient calls: "Why does my portal show someone else's lab results?" You have 60 days to decide whether you owe HHS a breach notification.*

THE REALITY

Healthcare is the most-targeted ransomware sector in the country. The average healthcare breach costs $9.77 million — and the original entry point is almost always one employee clicking one email.

NO LEGAL JARGON. JUST WHAT YOUR PRACTICE HAS TO DO.

What HIPAA actually requires — in plain English.

Most practices assume HIPAA compliance is the EHR vendor's job. It isn't. **HIPAA holds your practice accountable for the controls on your side of the system** — who logs in, who can see what, what happens when someone leaves, and what you do when something goes wrong. Here's what that means in plain English.

WHAT HIPAA ACTUALLY REQUIRES — IN PLAIN ENGLISH

Control Who Logs In

Every staff member has their own login. No shared passwords. MFA on every account. Off-board accounts the day someone leaves.

Keep Records Of Who Did What

Your EHR must log every access to patient records. You need to be able to produce that log if HHS asks.

Encrypt Patient Data

Patient records must be encrypted when stored and when sent — email, text, and data on laptops and USBs.

Have A Written Response Plan

If a breach happens, you need a written plan with named people responsible. 'We'll figure it out' is not a plan.

Sign Agreements With Every Vendor

Every company that touches patient data — your IT firm, your billing company, your fax service — needs a signed BAA.

Do An Annual Risk Review

Once a year, document your risks and what you did about them. This is the evidence OCR asks for first.

THE MOST EXPENSIVE MISUNDERSTANDING IN HEALTHCARE IT

Your EHR being HIPAA-compliant does not mean your practice is HIPAA-compliant. HIPAA is a shared-responsibility model. The EHR is responsible for the controls inside their platform. **Your practice is responsible for everything around it** — the workstations, the network, the email, the off-boarding when a doctor leaves, and the Business Associate Agreement with every vendor who touches patient data. A compliant EHR and a non-compliant practice is still a violation.

WE DON'T LEARN YOUR SYSTEMS ON YOUR TIME

Your systems. Already familiar.

Most IT companies treat medical software like any other application. They learn your EHR, your billing system, and your patient messaging platform after they're onboarded — on your time. We've already worked in the systems South Florida practices run. We know how Epic, athena, eClinicalWorks, and the billing platforms connect. We know which telehealth platforms carry a BAA and which ones don't.

SYSTEMS WE ALREADY KNOW — NO LEARNING ON YOUR TIME

EHR / EMR
Epic · Cerner · athenaOne
eClinicalWorks · NextGen
AdvancedMD · ModMed

Billing & Practice Mgmt
athena IDX · AdvancedMD
Kareo · Tebra · Waystar
Change Healthcare

Telehealth
Doxy.me · Zoom Healthcare
Updox · Spruce

Secure Messaging
Klara · TigerConnect
OhMD · Spruce
Solutionreach

HIPAA-Safe Fax
SRFax · Updox
eFax Corporate (BAA)
mFax

Network & Security
Fortinet · Cisco Meraki
CrowdStrike / SentinelOne
Duo · Imprivata SSO

A QUESTION DOCTORS DON'T ALWAYS THINK TO ASK

Does your IT firm know whether your telehealth platform, your patient messaging app, and your eFax service have signed a Business Associate Agreement with your practice? If not, **every message sent through those platforms is a potential HIPAA violation** — regardless of how secure the platform claims to be. We check every vendor. We don't assume.

THIS WILL HAPPEN. THE QUESTION IS WHETHER YOU'RE READY.

The EHR went down at 8 a.m. 12 patients are scheduled at 8:30.

Every practice eventually faces EHR downtime. It might be your internet connection, the EHR vendor's servers, or a ransomware attack. When it happens without a plan, the result is the same: **no charts, no schedule, no e-prescribing, no billing — and a waiting room full of patients who don't understand why their appointment isn't happening.**

Reverting to paper during a downtime event is both a HIPAA risk and a revenue hole. Paper notes get lost. Medications get missed. Charges don't get captured. Every hour of unplanned downtime costs a medical practice significantly in lost billing and staff time.

A real downtime plan isn't complicated — but it has to exist before you need it. The practices that handle EHR outages well have three things in common: a redundant internet connection, an offline-charting fallback that staff have actually practiced, and an IT firm that answers the phone when it happens.

WHAT A REAL DOWNTIME PLAN INCLUDES

Four things your practice needs ready before it happens.

01 REDUNDANT INTERNET
A backup connection that kicks in automatically when the primary goes down.

02 OFFLINE-CHARTING FALLBACK
A documented process for seeing patients without the EHR — practiced in advance, not invented on the spot.

03 SEPARATE CLOUD BACKUP
Your own backup of EHR data — separate from whatever the vendor provides, tested by actually restoring.

04 A PHONE NUMBER THAT ANSWERS
An IT firm that picks up — not a ticket portal with a 48-hour SLA while twelve patients are waiting.

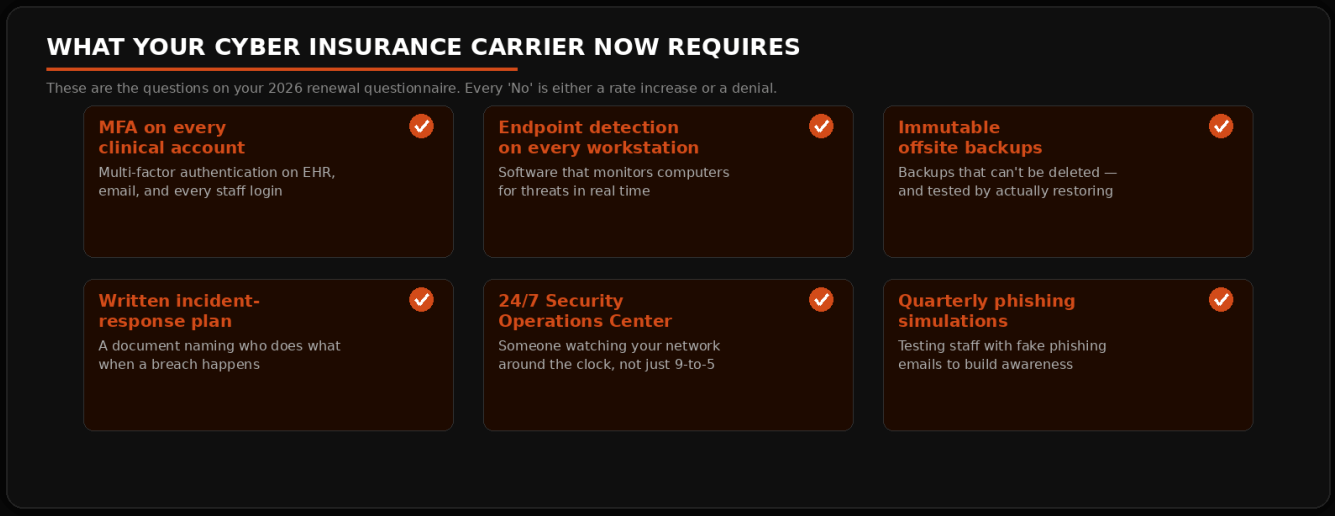
OUR COMMITMENT

Our target recovery time for critical systems is under 4 hours. And we built the plan before you needed it — not after.

YOUR RENEWAL QUESTIONNAIRE IS GETTING HARDER EVERY YEAR

The cyber insurance checklist your practice must pass.

Cyber insurance carriers started paying out enormous healthcare claims — and they changed their requirements to match. Your 2026 renewal questionnaire has six items that every practice must now say "yes" to. **Every "no" is either a rate increase, a coverage exclusion, or a denial.** Here's what they're asking and what it actually means.



THE GOOD NEWS

The same controls that satisfy your cyber insurance carrier mostly satisfy HIPAA Security Rule too. MFA, endpoint detection, tested backups, a written incident-response plan, and a 24/7 SOC — we deploy all of them, and we produce the documentation your carrier asks for so **renewal is never a panic week.**

FLAT RATES. NO SURPRISES.

What it actually costs.

RRG managed services are priced per device at a flat monthly rate: **$300/month per server, $150/month per workstation, and $5/month per mobile device.** These are managed IT prices only — cybersecurity services are priced separately. No per-incident charges, no overtime surprises, no invoice you didn't expect.

RRG MANAGED IT — MONTHLY PRICING

Per-device flat rate. Managed IT only — cybersecurity is priced separately.

$300 /month	$150 /month	$5 /month
PER SERVER	**PER WORKSTATION**	**PER MOBILE DEVICE**
EHR servers, billing systems, domain controllers, backups	Front-desk PCs, provider laptops, clinical computers	Tablets, phones under practice MDM management

WHAT SHOULD BE INCLUDED

Security patches. Antivirus and firewall monitoring. Backup verification. Spam filtering. Workstation and server health monitoring. Network documentation updated quarterly. BAA signed and on file.

WHAT'S OFTEN NOT INCLUDED

Hardware. EHR software licenses. Special projects (e.g. new office buildout). Cybersecurity services (priced separately). Ransomware recovery. Annual HIPAA risk assessment. Always get this list in writing before signing.

GET IN WRITING

If ransomware hits your practice, recovery can take hundreds of hours. Before you sign anything, confirm IN WRITING who pays for that — you, or them.

CUSTOMER SERVICE · Q1–Q5

Ask these before you sign anything.

These are the questions you — as the physician and practice owner — should ask before your practice signs an IT contract. You carry the liability. You should own the conversation. Write down the answers. If they hedge, that's the answer.

Q1 **When something breaks, how do I get help — do I call, email, or submit a ticket?**

You should be able to do all three. In a medical practice, a front-desk staff member can't navigate a support portal when the check-in system is down and patients are waiting. **We answer by phone, email, or ticket — whatever is fastest for you in the moment.**

Q2 **What are your actual hours? What happens if the EHR goes down at 7 a.m.?**

Our office hours are 9 a.m.–5:30 p.m., Monday–Friday. **After-hours emergency support is available for critical outages** — the kind that prevent your practice from seeing patients. Ask any IT firm to define "emergency" in writing before you sign. Vague language costs you on the day it matters most.

Q3 **Do you sign a Business Associate Agreement? What does that actually mean?**

A BAA (Business Associate Agreement) is a legal document that makes your IT firm accountable under HIPAA for how they handle your patient data. **If your IT firm accesses your systems — your EHR, your network, your email — without a signed BAA, your practice is already in violation.** We sign one with every client before we touch anything.

Q4 **Will I have one person to call — or will I re-explain our practice every time?**

Without a dedicated contact, someone in your practice re-explains your EHR, your locations, and your setup to a different person every time they call. **Our clients have a dedicated account manager who knows your practice** — so you're never starting from scratch.

Q5 **How do you handle a new doctor joining — or one leaving?**

A new provider needs EHR access, email, billing software, and MFA set up before they see their first patient. A departing provider's access needs to be removed the same day they leave. **We provision and off-board through a single process — so nothing gets missed and no old login stays active.**

IT MAINTENANCE · Q6–Q12

What's actually in the contract.

"Everything included" contracts almost never are. Know before you sign what triggers a bill you didn't expect.

Q6 Are you watching our systems, or waiting for us to call when something breaks?

Proactive monitoring means catching a server problem before the EHR goes down during office hours — not after. Ask specifically: "Do you monitor our systems 24 hours a day, or do you respond when we report a problem?"

Q7 If ransomware hits us, is recovery included — or is that an extra bill?

Recovery from a serious ransomware attack can be hundreds of hours of work. **Get the answer in writing before you sign.** Also confirm whether unlimited help desk, email support, billing software support, and multi-location coverage are included or extra.

Q8 Do your engineers know healthcare software — or will they be learning on our time?

Ask if they've worked with your specific EHR. A generalist IT firm that treats Epic the same as QuickBooks will cost your practice time and frustration. We've worked in the EHR and billing platforms your practice uses — we don't learn on your dime.

Q9 What happens when your tech goes on vacation or leaves your company?

A one- or two-person IT shop creates single points of failure. **We have a full team of certified engineers** — including Fortinet-certified network specialists. Your practice doesn't lose support because one person is on PTO.

Q10 Do you document our network — and do we get a copy?

Yes — at no extra charge, updated quarterly. If you ever change IT firms, you walk away with a complete record of your network. No one holds that documentation hostage.

Q11 Will we meet regularly to review what's working and what needs attention?

We meet quarterly with you — the physician or practice owner — not just whoever handles the phones. Budget, upcoming compliance obligations, anything that's been an issue. In plain English, so you can make informed decisions without needing a technical background.

Q12 How do we leave if it isn't working?

We start every new client with a **3-month trial period.** If you're not satisfied at any point during those 90 days, you can walk away — no penalties, no fines. Our 97% retention is earned, not enforced.

HIPAA & SECURITY · Q13–Q17

Questions that separate healthcare IT from generic IT.

Any IT firm can set up a computer. Not every IT firm understands HIPAA, has worked with EHR systems, or knows what a BAA is. These questions find out the difference.

Q13 **Can you explain HIPAA compliance in terms of what you do — not just what it is?**

A firm that knows healthcare IT can tell you specifically: we configure MFA on every account, we set up audit logging in your EHR, we encrypt your laptops, we off-board accounts same-day, we conduct an annual risk analysis, and we sign a BAA. **If they describe HIPAA in general terms but can't explain their specific practices, they haven't done this before.**

Q14 **What do you do to protect every computer in our office?**

Every workstation your practice uses — front desk, provider laptops, nursing stations — needs its own security software that monitors for threats in real time. This is called endpoint detection. **"We have antivirus" is not sufficient for a HIPAA-covered practice.** Ask what they specifically run on every machine.

Q15 **If your mistake contributes to a HIPAA breach, what insurance do you carry?**

If an IT firm's negligence contributes to a patient data breach, they should be able to cover their share of the liability. **RRG carries cyber liability, errors & omissions (E&O) insurance, and workers' compensation.** Ask to see the policy. Any reputable IT firm will show it to you.

Q16 **Who checks your work — who audits your own security?**

An IT firm that only audits itself is like a doctor reading their own medical results. **We're audited by Galactic Advisors — an independent firm.** Ask any IT company who holds them accountable when something goes wrong on their end.

Q17 **Are our staff being tested for phishing — the way real attacks come in?**

Most healthcare breaches start with one employee clicking one email. **Quarterly phishing simulations** — sending fake phishing emails to your own staff — are now required by most cyber insurance carriers and recommended by HIPAA guidance. Your staff will click something. The question is whether it's a test or the real thing.

BACKUPS & DISASTER RECOVERY · Q18–Q21

The day after the ransomware note.

What does your practice look like the morning after a ransomware attack? That answer is determined by decisions made months before — not hours after.

Q18 **If ransomware hits us tonight, when can we see patients again?**

The honest answer to this question tells you everything. A real IT firm with a real plan will say: your systems go to a cloud backup within hours, staff can keep working, and full restoration is complete within a documented recovery-time window. **Ask them to name a specific number of hours** — not "as quickly as possible." We target under 4 hours for critical systems.

Q19 **How do we know our backups actually work — not just that the backup ran?**

A backup that runs every night but has never been tested for restoration is not a working backup. **We test backups by actually restoring from them** — not by checking that the job completed. Quick test you can run today: ask your IT firm to restore three files from last week's backup right now. If they can't do it quickly, you have a problem.

Q20 **If a hurricane takes out power and internet for three days, how do we operate?**

South Florida is in the Atlantic hurricane corridor. This is not a hypothetical. **Ask specifically how their existing healthcare clients operated during recent major storms.** Ask to speak to one of them. The answer to this question matters more here than almost anywhere else in the country.

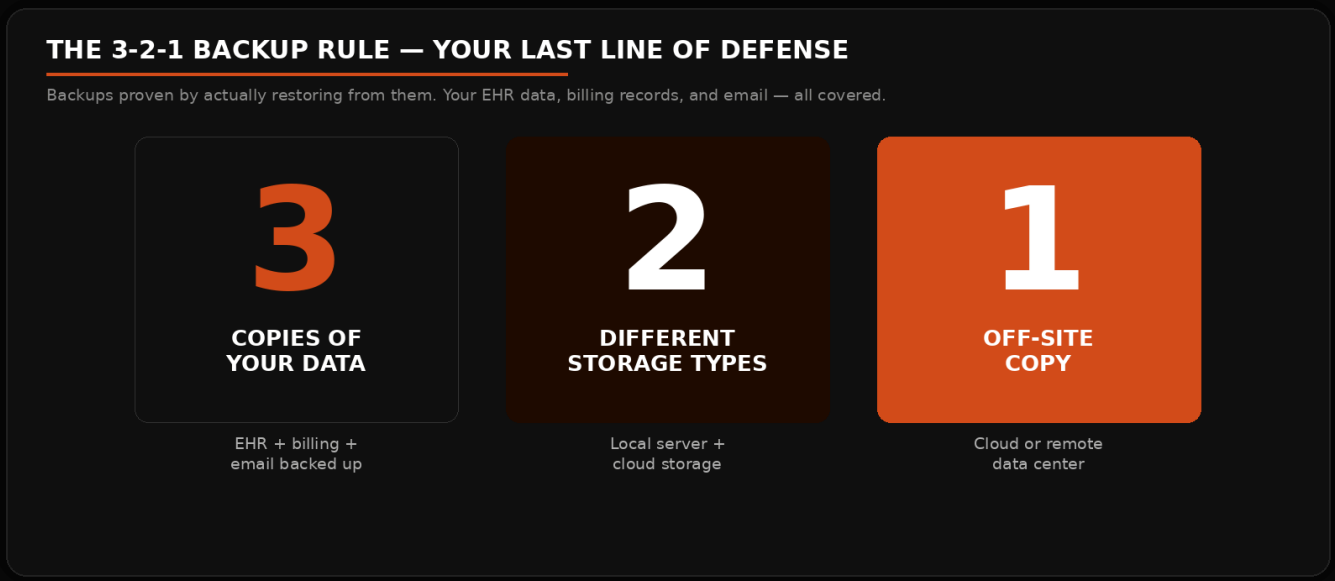
Q21 **What does onboarding look like — especially if we're leaving a bad IT situation?**

The most common engagement we run in healthcare is taking over from a situation where the previous IT person left and documented nothing. **Our first two weeks: we find every account, every device, every login, every vendor contract.** We rotate passwords, enroll MFA, and document everything. You have a real IT operation, in writing, that doesn't walk out the door when one person leaves.

RANSOMWARE, HURRICANES, AND THE BACKUP RULE

Your last line of defense is your backup.

Every practice that paid a ransom had one thing in common with the ones that didn't: they both got hit. The difference was the backup. **A tested, immutable, offsite backup is the difference between a bad week and a catastrophic one.** "Immutable" means the backup can't be deleted — even by ransomware that encrypts everything else. "Tested" means someone actually restored from it recently.



We get practices through a complete ransomware-readiness program — backups, MFA on every account, endpoint detection on every workstation, and a written incident-response plan with named people — in **60 to 90 days, without disrupting your operations.**

WHAT "RANSOMWARE READY" ACTUALLY MEANS

MFA on every account. Endpoint detection on every workstation. Immutable offsite backups tested by restoring. Written incident plan with named roles and a clear escalation path to you as the physician. 24/7 security monitoring from our SOC.

WHAT HAPPENS IF YOU'RE NOT READY

The ransom demand — often $40K to $400K for a medical practice. Recovery labor — often hundreds of hours. HHS notification if PHI was accessed. Potential OCR investigation. Business interruption while systems are rebuilt. Cyber insurance claim — if coverage applies.

YOUR NEXT STEP

30 minutes.
No jargon. No pitch.

Call our office and reference this guide. We'll have an honest conversation about your EHR uptime, your HIPAA exposure, your cyber insurance readiness, and what's actually breaking in your practice right now. If we're a fit, we'll schedule a full IT assessment — at no charge, with no obligation.

AFTER OUR FREE CALL, YOU'LL KNOW AS THE PHYSICIAN:

IF YOUR HIPAA EXPOSURE IS ACTUAL OR THEORETICAL
Not just what the policy says — what's real

WHICH ACCOUNTS STILL HAVE ACCESS THAT SHOULDN'T
Old staff, departed providers, vendors

IF YOUR BACKUPS WILL ACTUALLY RESTORE
EHR, email, billing data tested

YOUR CYBER INSURANCE GAP LIST
Exactly what you need to meet renewal requirements

WHERE YOU'RE OVERPAYING OR UNDERSERVED
Without the jargon. In plain English.

BOOK A DISCOVERY CALL

(844) 919-8534

Reference this guide for your free practice assessment. rrgnetworks.com/industries/healthcare/

CHOOSE I.T. WISELY.

Ready to talk?
Let's start.

A free, 30-minute call for physicians and practice owners. No obligation. No pitch. No jargon. An honest conversation about your HIPAA exposure, your EHR uptime, your cyber insurance readiness — and what good IT looks like when you're a doctor who just wants to see patients.

---

(844) 919-8534

rrgnetworks.com/industries/healthcare/

12343 SW 132nd Court · Miami, FL 33186