

Why a Healthcare Practice Should Consider AdvancedBITS

What a managed IT partner can and cannot do for a healthcare practice, what the evidence shows, and how to hold any provider accountable

By AdvancedBITS | Business IT Solutions • About 10 minutes to read

Quick answer: why would a healthcare practice consider a managed IT partner?

A healthcare practice should consider a **managed IT partner** when it cannot show that its patient data is protected, its systems can be restored, and someone is watching them after hours. HIPAA already expects a practice to assess risk to electronic patient information and act on what it finds, and federal regulators have been settling cases with small practices that never did. A managed partner supplies the team, the documentation, the monitoring, and the recovery testing, but it does not take over the practice's legal responsibility, and nothing makes a practice immune to attack. This paper explains when AdvancedBITS is worth a look, what the evidence supports, and when it is not the right answer.

A medical, dental, behavioral health, or specialty practice runs on a handful of systems: the electronic health record, scheduling and billing, Microsoft 365, a patient portal, and the devices people use all day. When any of them stops, patients wait and revenue stops. When any of them leaks, the practice owes its patients and its regulator an explanation.

We make the case on evidence a skeptical administrator can check, and we say where the evidence ends. This page covers the decision. For what we do day to day, see [Managed IT, Cybersecurity, and AI Readiness for Healthcare Practices](#), for an example of an engagement, see [Healthcare Provider Strengthens Security, Compliance, and Patient Care Through Strategic Technology](#), and for AI, see [Healthcare Technology and AI Operating Model](#).

A note on who wrote this

AdvancedBITS is a managed IT provider, so this paper makes a case for hiring one. We have tried to make it testable: statistics are linked and labeled by strength, reasoning is marked as reasoning, and we say when a managed partner is not the right answer. AdvancedBITS is not a law firm, does not certify HIPAA compliance, and does not replace your compliance officer, counsel, or clinicians. Your practice remains responsible for its own HIPAA obligations.

General information about technology risk. It is not legal or compliance advice. AdvancedBITS quotes no client results in this paper.

Why is a healthcare practice's IT hard to keep running and protected?

Short answer: Healthcare is a steady target, the damage reaches small practices through their vendors, and a breach costs more here than in any other sector. Each statistic appears once, here.

Finding	Source	Strength and limits
For 2025, 772 large healthcare data breaches (500 or more people) were listed on the HHS breach portal as of June 2026, a record, exposing the records of 139,721,832 people. That count is expected to rise as investigations conclude.	HIPAA Journal, largest breaches of 2025 , built from the HHS Office for Civil Rights portal.	Trade publication reading a federal register. Another tracker counted more filings at a different date, so recheck the portal for the current number.
HHS's Office for Civil Rights says hacking and ransomware are the most frequent type of large breach reported to it.	HHS press release, April 23, 2026 .	Primary. A statement from the regulator.
The 2024 attack on Change Healthcare exposed an estimated 192.7 million people. HIPAA Journal reports attackers entered through a remote access portal with stolen credentials and no multifactor authentication.	HIPAA Journal .	Trade publication. The entry-point detail is secondary reporting.
In an informal AMA survey after that attack, 80% of respondents lost revenue from unpaid claims, 85% committed extra staff time, 55% used personal funds to cover expenses, and 31% could not make payroll. Most of the roughly 1,400 respondents were in practices with fewer than 10 physicians.	AMA informal survey, March 26 to April 3, 2024 .	Primary AMA document, but an informal convenience sample, so read it as directional.

Finding	Source	Strength and limits
Healthcare was the costliest sector for a data breach for the 13th year running, at \$6.64 million on average, down 10.5% from \$7.42 million. The global average across industries was \$4.99 million.	Becker's, citing IBM's 2026 Cost of a Data Breach Report; IBM report page.	IBM and Ponemon, 602 breached organizations, all sizes. Averages are skewed by large breaches, so a small practice's cost will differ.

What does HIPAA expect of a practice's technology?

Short answer: That the practice assesses the risks to its electronic patient information, act on what it finds, and be able to show the work. Federal regulators are enforcing exactly this, including against small organizations.

The Security Rule's **risk analysis** requirement asks every covered entity and business associate for an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information. A **business associate** is an outside party that creates, receives, maintains, or transmits patient information on a covered entity's behalf, and it needs a written business associate agreement before it touches that information.

What regulators and HHS say	Source	What it means for a practice
On April 23, 2026, OCR announced settlements with four regulated entities after separate ransomware investigations, collectively affecting over 427,000 people. They paid \$1,165,000 in total and agreed to corrective action plans monitored for two years. The release marks 19 ransomware investigations and 13 Risk Analysis Initiative investigations completed.	HHS press release, April 23, 2026.	Enforcement is active, and a ransomware incident can open an inquiry into the basics.
On June 18, 2026, OCR announced a settlement with a group health plan, calling it its 20th ransomware enforcement action and 14th in the Risk Analysis Initiative.	HHS press release, June 18, 2026.	The initiative is continuing. Its cases include group health plans and other small entities.
When a covered entity uses a cloud provider to store electronic patient information, the provider is a business associate, even if it holds only encrypted data and has no key.	HHS guidance on HIPAA and cloud computing.	Do not assume a vendor with limited access is outside HIPAA. Ask for the agreement.
HHS answers “can business associates self-certify or be certified by a third party as compliant with HIPAA?” with “No.”	HHS business associate FAQ.	There is no HIPAA certification for a provider, so treat “HIPAA certified” claims with caution.
HHS proposed updates to the Security Rule in December 2024, the first in more than a decade. HIPAA Journal reports the final rule has slipped to July 2027 on the federal regulatory agenda. The current rule remains in effect.	HHS, HIPAA Security Rule NPRM; HIPAA Journal, July 8, 2026.	Do not wait for the final rule. Today's requirement is already being enforced.

What does a managed partner add that a practice often lacks?

Short answer: Coverage across hours, specialization, documentation, and evidence, and each item below should come with something you can read.

This table is AdvancedBITS reasoning, drawn from what practices commonly tell us. It is not research. The last column is how you can check each claim.

Area	Common gap	What managed support adds	How you verify it
Risk analysis and risk management	No current, written risk analysis, or one that was never acted on.	Help gathering the inventory, running or supporting the analysis, and tracking remediation. The practice's compliance lead owns the result.	A dated analysis and a remediation list with owners.
Identity and remote access	Multifactor authentication covers email but not the EHR portal, VPN, vendor accounts, or administrators.	MFA and conditional access across systems, separate administrator accounts, and periodic access reviews.	Coverage reports by system and user.
Endpoints, email, and patching	Patches wait for a quiet day, staff cannot tell phishing from a real request, and email is the main door.	Endpoint protection, email filtering, scheduled patching around clinic hours, and staff training.	Patch-age and phishing-report summaries.

Area	Common gap	What managed support adds	How you verify it
Microsoft 365 permissions	Old sites and shared folders let people reach patient information they do not need.	Permission and sharing review, labels, and site ownership.	An access review record.
Backup and recovery	Backups run, but no one has restored the practice's data against a clock.	Monitored backups with an offline or immutable copy, and scheduled restore tests.	Restore test records, with times.
Downtime readiness	No plan for seeing patients when the EHR, clearinghouse, or internet is down.	A written downtime plan and a rehearsal with clinical and front-desk staff.	A tabletop record with the date and lessons.
Vendor and business associate tracking	No single list of who touches patient data and under what agreement.	An inventory of vendors with access to systems, with agreements and review dates.	The list itself.
Documentation and key-person risk	One administrator holds the passwords and the knowledge.	Current diagrams, inventories, runbooks, and shared coverage.	Documents readable without the provider in the room.

Who owns what: the practice, the vendors, and AdvancedBITS?

Short answer: The practice owns its compliance and clinical decisions, vendors own their own hosted systems and devices, and a managed partner owns the practice's IT environment alongside it.

Party	Typically owns	How AdvancedBITS works with them
Practice (administrator, compliance lead, physicians)	HIPAA responsibility, policies, risk acceptance, clinical decisions, and workforce conduct.	Informs and documents. Does not make clinical or legal decisions and does not take over compliance leadership.
EHR and billing vendors, clearinghouses	Their own hosted systems and security, under their contracts and business associate agreements.	Coordinates, tracks the agreements, and helps the practice prepare for their outages.
Medical device manufacturers and biomedical staff	Clinical devices, their software, and their maintenance.	Covers the IT side of the network boundary. Does not scan or change clinical devices without the owner's approval.
AdvancedBITS	The practice's business IT environment under a written agreement: endpoints, Microsoft 365, identity, backup, monitoring, documentation, and reporting.	Manages, secures, documents, and reports, fully or alongside the practice's own IT staff.

Where a practice's systems hold patient information, a business associate agreement should be in place before any provider, including us, touches them.

What should a practice ask any IT partner before hiring?

Short answer: Ask for the agreement and the evidence before access begins, not after.

- Will you sign a business associate agreement before you touch any system that holds patient information, and who are your subcontractors?
- Who at your company can reach our systems, how is that access logged, and how is it removed?
- Can we read your SOC 2 report? What is its period, scope, and exceptions? (The [AICPA](#) says SOC services should be thoroughly evaluated, and a SOC 2 report is not a HIPAA certification.)
- Who owns our risk analysis, and what will you do to help produce and maintain it?
- How do you handle an incident at 2 a.m., and how quickly will you tell us so we can meet our own notification duties?
- Can you show a recent restore test, with the time it took, for a comparable practice?
- What is our plan if the EHR or clearinghouse is down for a week?
- What are the exit terms, and who owns our documentation, configurations, and data when we leave?
- Can we speak with practice of our size and type?

How can a practice measure whether managed IT is working?

Short answer: Baseline first, then re-measure at 90 days, using your own numbers.

AdvancedBITS suggests a 90-day first cycle: discover and document in days 1 to 30, close the highest-risk gaps in days 31 to 60, then test restores, rehearse downtime, and report in days 61 to 90. The plan is an illustrative AdvancedBITS framework, not a published standard. This composite example shows the sequence: [Healthcare Provider Strengthens Security, Compliance, and Patient Care Through Strategic Technology](#).

Measure	Baseline at day 1	Check at day 90
Risk analysis	Whether one exists, how old it is, and whether findings were acted on.	A current, dated analysis and a remediation list with owners.
Multifactor authentication coverage	Share of users, administrators, vendor accounts, and remote access covered.	Gaps closed, and exceptions documented.
Former-workforce accounts	Accounts still enabled for people who left in the last 12 months.	None known, with a record for each departure.
Restore time	Whether critical data has been restored against a clock.	A completed restore test, with the time it took.
Vendors with patient-data access	A list, with agreements and review dates.	The list is complete and each entry has an owner.
Downtime readiness	Whether a written plan exists and has been rehearsed.	A tabletop completed, with the date and lessons recorded.
Staff training	Who has had security awareness training this year.	Completion records and a phishing-report process.

When is a managed partner not the right answer?

Short answer: When no one will own compliance, when a strong in-house team needs support and not a handover, or when the main exposure is something an IT partner does not cover.

- **A capable in-house administrator may want co-managed IT.** The provider takes defined work, such as after-hours monitoring and backup testing, and your staff keeps control.
- **Accountability does not transfer.** A provider can run controls and keep records, but the practice still owns its HIPAA obligations and must review what it is told.
- **Clinical devices and EHR hosting need their owners.** An IT partner should say so and coordinate with the device manufacturer or EHR vendor, not claim to cover them.
- **Very small practices can start free.** HHS's [405\(d\) program](#) offers no-cost cyber hygiene resources, including its Health Industry Cybersecurity Practices publications, and many practices can do real work with them first.
- **No one can promise you will not be attacked.** Be wary of any provider, including us, that does.

Why AdvancedBITS?

Short answer: We pair managed IT experience with documentation and reporting you can read, and we are plain about our limits. The points below are company-reported, so verify them the way you would any vendors.

- **11+ years** of managed services experience.
- **Independently audited** to the SOC 2 Type II standard. Read the report and remember it is not a HIPAA certification.
- **Managed or co-managed**, so your in-house staff keeps control if you want it.
- **Microsoft 365, identity, and backup depth.** Core work, not add-ons.
- **Measured.** A baseline now, a re-measurement at 90 days, and regular reports after that.
- **Plain limits.** We do not guarantee outcomes, we do not give legal advice or certify HIPAA compliance, we do not replace your compliance officer or clinicians, and we do not quote client results without documented evidence.

For what we do day to day, see [Managed IT, Cybersecurity, and AI Readiness for Healthcare Practices](#). For AI, see [Healthcare Technology and AI Operating Model](#) and [AI in Healthcare: A Case Study in Responsible Workflow Modernization](#).

Frequently Asked Questions

Should a healthcare practice hire a managed IT provider?

Often yes, when no one can show current risk analysis, tested backups, and after-hours monitoring, or when technology depends on one person. Practice with a capable in-house administrator may prefer co-managed IT. Either way, choose a provider that signs a business associate agreement, documents its work, and reports with evidence.

What does a managed IT provider do for a medical practice?

A managed IT provider runs, secures, backs up, and documents a practice's technology under a written agreement, either fully or alongside in-house staff. Typical work includes help desk support, security monitoring, Microsoft 365 administration, backup and restore testing, vendor coordination, and regular reports.

Does a managed IT provider make a practice HIPAA compliant?

No. HIPAA responsibility stays with the practice, and HHS says a business associate cannot self-certify or be certified as compliant. A provider can help assess risk, run controls, and keep records, which supports compliance. Your compliance lead and counsel decide what the practice must do.

Does an IT provider need a business associate agreement?

If the provider creates, receives, maintains, or transmits patient information on the practice's behalf, it is a business associate and needs a written agreement. HHS says even a cloud provider holding only encrypted data is one. Ask for the agreement before the provider touches any system and ask counsel to review it.

Why do small practices get enforcement actions?

OCR's Risk Analysis Initiative targets failures to assess risk to electronic patient information, and its cases include small and mid-sized entities. A breach, often a ransomware or phishing incident, opens the inquiry, and the missing or outdated analysis can drive the outcome. A current analysis you can produce on request changes that conversation.

What is the difference between managed and co-managed IT?

With fully managed IT, the provider runs the practice's technology day to day. With co-managed IT, the provider works alongside in-house staff and takes on defined work, such as after-hours monitoring, patching, backup testing, or reporting, while the internal team keeps control. Practices choose the model that fits their staff and risk.

What should a practice do if the EHR or clearinghouse goes down?

Have a written downtime plan that names who decides to switch to paper, how patients are seen and billing is recorded, who contacts the vendor, and how data is entered afterward. Rehearse it with clinical and front-desk staff. The 2024 Change Healthcare outage showed how quickly a vendor outage reaches a practice's payroll.

Is there proof that managed IT reduces breaches at medical practices?

We did not find a published study that measures medical practices before and after hiring a managed IT provider. The evidence concerns specific controls and what regulators enforce. The practical test is your own baseline and a re-measurement at 90 days, using restore time, multifactor authentication coverage, and a current risk analysis.

Does AdvancedBITS provide legal advice or certify HIPAA compliance?

No. AdvancedBITS provides technology, security, and planning services. Your counsel and compliance lead decide which laws and contract terms apply to your practice, and no provider can certify that a practice is HIPAA compliant.

Closing perspective

A healthcare practice does not need exotic technology to be safer. It needs to know what it holds, who can reach it, how fast it can be restored, and who acts when something goes wrong, and it needs to be able to show that. Hiring a managed partner is a reasonable way to get there, but it moves the work and not the responsibility. Test the claims, ask for the agreement and the evidence first, and measure the difference against your own baseline.

See where your practice stands before you decide

A specialist will review your technology, security, backups, and vendors and show you where a managed partner would help, and where it would not. No cost, no obligation.

Schedule Your Complimentary Healthcare Technology Assessment

Call 561-300-3015 | Email sales@advancedbits.com

Sources

Several figures come from trade publications or informal surveys, and IBM's average is skewed by large breaches. The risk-analysis and business-associate points come from HHS. The two tables of what a partner adds and who owns what are AdvancedBITS's reasoning, and no client results are quoted.

- Breaches and costs: [HIPAA Journal, largest breaches of 2025](#); [HIPAA Journal on Change Healthcare and the Security Rule](#); [AMA informal survey](#); [Becker's on IBM 2026](#); [IBM Cost of a Data Breach Report 2026](#)
- Regulation and enforcement: [HHS, April 23, 2026](#); [HHS, June 18, 2026](#); [HHS Security Rule NPRM](#); [HHS cloud computing guidance](#); [HHS business associate FAQ](#)
- Resources: [HHS 405\(d\) program](#); [AICPA SOC services](#)
- AdvancedBITS: [Managed IT, Cybersecurity, and AI Readiness for Healthcare Practices](#); [Healthcare Provider Strengthens Security, Compliance, and Patient Care Through Strategic Technology](#); [Healthcare Technology and AI Operating Model](#); [AI in Healthcare: A Case Study in Responsible Workflow Modernization](#)

Secure. Compliant. Outcome-Focused. | sales@advancedbits.com | www.advancedbits.com | 561-300-3015