WHAT TO ASK BEFORE YOU SIGN: A HEALTHCARE LEADER'S GUIDE TO MANAGED IT AGREEMENTS

MAINSTAY TECHNOLOGIES

MAINSTAY
TECHNOLOGIES

Technology problems in healthcare rarely stay contained inside IT. A workstation that cannot connect, an EHR access issue, a failed backup, a delayed vendor response, or a compromised mailbox can affect scheduling, billing, patient communication, provider productivity, and compliance work. That is why any IT services agreement deserves close review before it is signed.

A strong agreement should tell leadership exactly what is covered, how urgent issues are handled, which systems receive support, how security controls are maintained, and what evidence will be available when someone asks for proof. A vague agreement leaves too much to interpretation, usually at the worst possible time.

This guide is written for **healthcare executives, practice administrators, operations leaders, finance leaders, compliance contacts**, and **internal IT leaders** who need to evaluate whether a Managed IT (or Co-managed IT) agreement fits the way their organization operates in the real world.

1. Start with the systems that keep the organization running

Questions to ask

- Which locations, users, devices, servers, and networks are covered?
- Are EHR, practice management, telehealth, imaging, billing, and patient communication systems addressed?
- Which applications are supported directly?
- Which applications remain the responsibility of the software vendor?
- Who coordinates support when an issue involves the MSP, the EHR vendor, the internet provider, and internal staff?
- Are clinical workstations, shared workstations, front desk workflows, remote users, and providers covered under the same support model?
- Are medical device connectivity issues included, excluded, or handled case by case?

Why this matters

Healthcare teams often experience technical problems as operational delays. A front desk login issue can slow check-in. A network problem can interrupt imaging access. A telehealth disruption can force staff to reschedule patients. An unclear vendor handoff can leave the practice waiting while each party points elsewhere.

The agreement should reduce that ambiguity. It should define who takes the lead, how issues are escalated, and where vendor responsibility begins.

2. Require a defined security baseline

Questions to ask

- Is multi-factor authentication included?
- Is endpoint detection and response included?
- Is antivirus management included?
- How are patches reviewed, approved, deployed, and reported?
- Are servers and workstations both covered?
- Is Microsoft 365 security configuration included?
- Are phishing simulations included?
- Is security awareness training included?
- Is vulnerability scanning included? How often?
- Is firewall administration included?
- Are VPN and remote access controls included?
- Is SIEM, SOC, or 24x7 monitoring included?
- Are security reports available for leadership, insurance, audits, or vendor questionnaires?

Why this matters

Healthcare organizations are often asked to show evidence of security controls. Requests may come from cyber insurers, auditors, business partners, regulators, board members, or parent organizations. If security services are described vaguely, leadership may have no reliable way to confirm which controls are active, which are monitored, and which are outside the service scope.

3. Review access control and user lifecycle management

Questions to ask

- Who submits access requests?
- Who approves new access?
- How are new users onboarded?
- How are role changes handled?
- How quickly are departing users disabled?
- Are stale accounts reviewed?
- Are privileged accounts monitored separately?
- Are shared accounts allowed?
- Is MFA required for remote access and key systems?
- Are access changes documented in tickets?
- Are access reviews included in the service?

Why this matters

Access issues create real exposure. A former employee with an active account creates avoidable risk. A provider without the right access loses productive time. Shared accounts weaken accountability. Privileged accounts without controls can increase the impact of an incident. Healthcare leaders should know how access decisions are made and documented.

4. Separate backup from recovery

Questions to ask

- Which systems are backed up?
- Are servers, files, Microsoft 365, cloud platforms, and databases included?
- Are EHR backups handled by the EHR vendor or by the Managed IT provider?
- How often do backups run?
- How often are restore tests performed?
- What recovery time objectives apply?
- What recovery point objectives apply?
- Are backup failures monitored and remediated?
- Are larger disaster recovery exercises included?
- Who sets restoration priorities during an outage?
- What is the process during a ransomware event?

Why this matters

A healthcare organization may be able to tolerate a brief outage in one system while another disruption affects patient care immediately. Recovery planning should reflect operational priority, system dependency, and patient-facing impact. A backup strategy that has never been tested can create false confidence.

5. Match support expectations to clinical operations

Questions to ask

- What are the standard support hours?
- How are urgent issues reported?
- What qualifies as a critical issue?
- Are response targets based on severity?
- How are clinic-wide outages handled?
- Is after-hours support included?
- Is onsite support included?
- Are provider issues prioritized differently from routine requests?
- Are phone system, internet, and EHR access issues escalated differently?
- Are SLA reports available?
- Are recurring issues reviewed with leadership?

Why this matters

A password reset and a clinic-wide network outage should never move through the same support path. The agreement should define urgency in terms that reflect healthcare operations. Leaders should also know how the provider handles patterns, such as repeated login problems, slow workstations, wireless dead zones, or recurring vendor issues.

6. Define the incident response role before an incident occurs

Questions to ask

- What incidents are covered under standard Managed IT support?
- How are suspected security incidents reported?
- Who triages the issue?
- Who contains the threat?
- Who preserves logs and evidence?
- Who communicates with leadership?
- Does the provider coordinate with cyber insurance or legal counsel?
- Is forensic investigation included?
- Is breach determination support included?
- Are incident reports included?
- Are tabletop exercises included?

Why this matters

During an incident, unclear roles slow the response. Technical teams may focus on containment while leadership needs timelines, scope, affected systems, insurer coordination, and evidence. The agreement should define how the provider supports the incident without overstating responsibilities that belong to legal counsel, privacy leadership, cyber insurance, or outside forensic specialists.

7. Make breach notification support explicit

Questions to ask

- How quickly will the provider notify the organization of a suspected security incident?
- What information will be included in the notification?
- Will the provider identify affected systems, users, mailboxes, devices, or files?
- Will logs be preserved?
- Will the provider support a breach risk assessment?
- Are internal notification timelines stricter than legal outer limits?
- Are incident timelines and technical summaries included?
- Who owns final breach determination?

Why this matters

The technical facts matter, but final breach decisions usually involve privacy leadership, legal counsel, and organizational leadership. A Managed IT provider can support the process with logs, containment details, timelines, affected asset information, and technical findings. That support should be spelled out in advance.

8. Clarify vendor coordination

Questions to ask

- Who maintains the vendor contact list?
- Who opens support tickets with application vendors?
- Who joins troubleshooting calls?
- Who tracks vendor follow-up?
- Who confirms whether the issue is local infrastructure, application configuration, user access, or vendor performance?
- Are upgrades and migrations included?
- Are interface issues included?
- Are medical device connectivity issues included?
- Are vendor management meetings included?

Why this matters

Staff usually need one accountable path to resolution. They should not have to determine whether the issue belongs to the MSP, EHR vendor, internet provider, phone vendor, or device vendor. A strong agreement gives the organization a coordination model.

9. Expect governance and useful reporting

Questions to ask

- Are regular service reviews included?
- Who attends those meetings?
- What reports are provided?
- Are ticket trends reviewed?
- Are unresolved risks tracked?
- Is patch compliance reported?
- Are backup results reviewed?
- Is endpoint protection status reviewed?
- Are MFA gaps reviewed?
- Are aging devices, warranty issues, and infrastructure risks documented?
- Is there a technology roadmap?
- Is evidence available for insurance, audits, and vendor questionnaires?

Why this matters

Healthcare organizations need to make budget and risk decisions before systems fail or controls are questioned. Governance meetings should help leadership see what needs attention, what has improved, and what decisions are pending. The reporting should be usable by nontechnical leaders.

10. Identify what is included, excluded, and project-based

Questions to ask

- What is included in the recurring monthly fee?
- What is billed hourly?
- What requires a project?
- Are onsite visits included?
- Is after-hours work included?
- Are Microsoft 365 changes included?
- Is cloud-to-cloud backup included?
- Are firewall replacements included?
- Are wireless upgrades included?
- Is network segmentation included?
- Are server migrations included?
- Is security consulting included?
- Are policy development and risk assessments included?
- Is advanced incident response included?
- Are third-party licensing costs separate?

Why this matters

Scope clarity helps leadership budget accurately and prevents surprise invoices. It also helps staff understand when a request is routine support, a security improvement, a compliance activity, or a separate project.

11. Address AI and automation (before staff create their own workarounds)

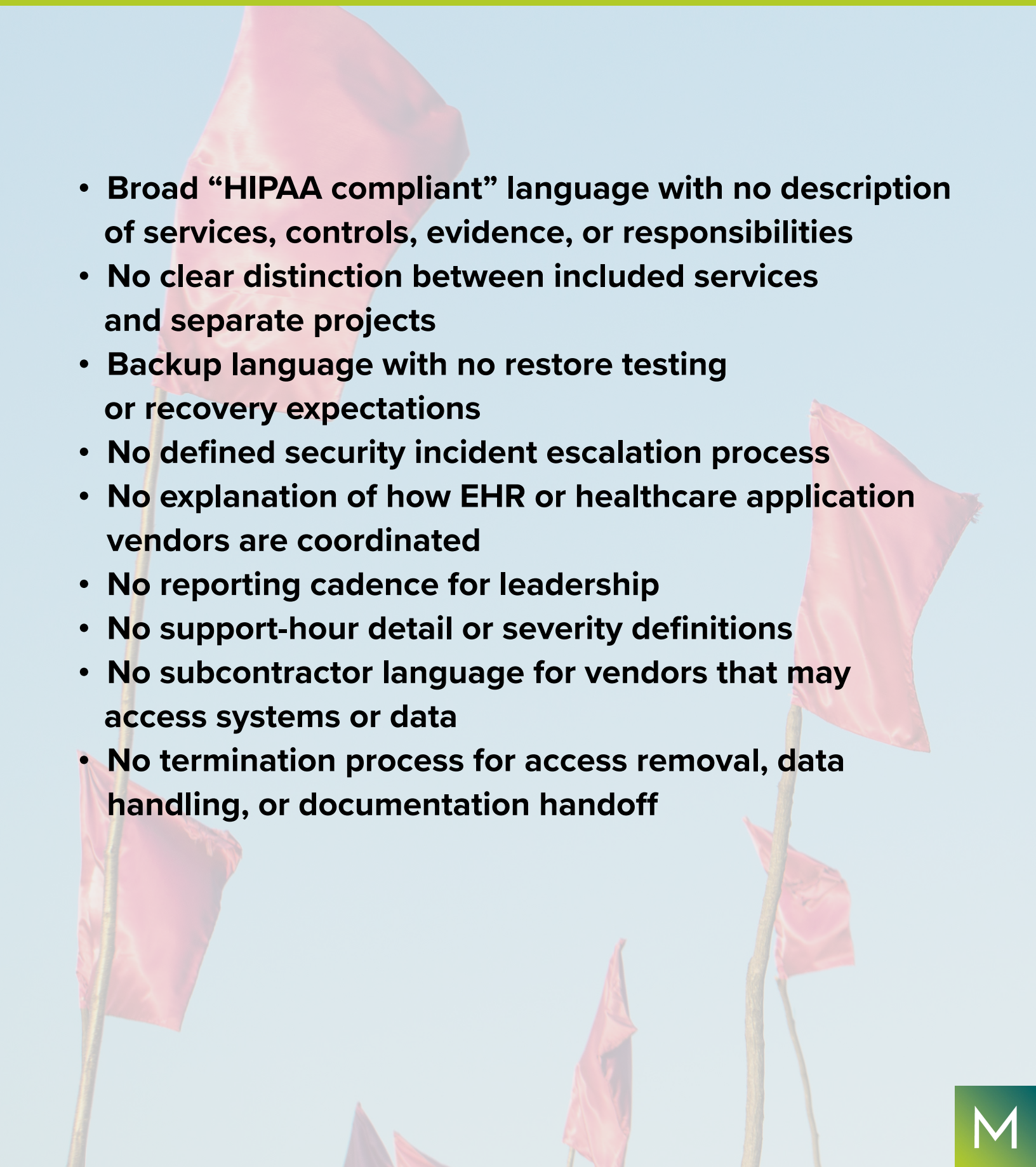
Questions to ask

- Are public AI tools allowed?
- Can staff enter PHI into any AI system?
- Are approved AI platforms documented?
- Who reviews AI tools before use?
- Are access controls, retention settings, and data handling terms reviewed?
- Are staff trained on safe AI use?
- Are automation workflows documented?
- Are AI-related support requests included in Managed IT scope?
- Who owns AI policy and enforcement?

Why this matters

Unmanaged AI use can expose sensitive data, create inconsistent workflows, and make it harder to know where information is going. Healthcare leaders should set guardrails before informal use becomes routine.

Red flags in a healthcare Managed IT agreement



- Broad “HIPAA compliant” language with no description of services, controls, evidence, or responsibilities
- No clear distinction between included services and separate projects
- Backup language with no restore testing or recovery expectations
- No defined security incident escalation process
- No explanation of how EHR or healthcare application vendors are coordinated
- No reporting cadence for leadership
- No support-hour detail or severity definitions
- No subcontractor language for vendors that may access systems or data
- No termination process for access removal, data handling, or documentation handoff

A practical agreement review checklist

Before signing, leadership should be able to answer these questions with *confidence*:

- Which clinical, administrative, and patient-facing systems are covered?
- Which systems remain under third-party vendor responsibility?
- Are PHI and ePHI handling responsibilities clear?
- Which security controls are included in the recurring service?
- Are MFA, endpoint protection, patching, email security, and backup monitoring addressed?
- Are backup testing and recovery expectations documented?
- Are support hours, urgent escalation paths, and onsite terms clear?
- Does the agreement explain what happens during a potential security incident?
- Are vendor coordination responsibilities defined?
- Will leadership receive reporting, risk visibility, and evidence?
- Are exclusions and project-based services easy to identify?
- Are AI and automation use cases governed before sensitive data is exposed?

Conclusion

A managed IT or co-managed IT agreement should give healthcare leaders a **clear operating model** for technology support, security controls, recovery, vendor coordination, and incident response.

The strongest agreements are **specific**. They define support expectations, address PHI responsibilities, show where evidence comes from, and make exclusions easy to understand.

The goal is an agreement that's aligned with your organization's real risk, real workflows, and real support needs.

Let's work together.

Scan the QR code
or visit us at mstech.com/contact
to get started.