



Medical Practice Vendor Safeguard Kit

KNOW WHAT TO ASK.

KNOW WHAT A GOOD ANSWER LOOKS LIKE.

A practical cybersecurity and HIPAA due-diligence guide
for healthcare practice leaders.

CYBERSECURITY-FIRST. HIPAA-GROUNDED.



Tailored IT. Hardened Security. [Connected Care.](#)



Look at both compliance and real-world security

Your practice relies on vendors for electronic health records, billing, managed IT, cloud services, phones, artificial intelligence tools, connected medical devices, and more.

HIPAA ASKS

Are we meeting the Health Insurance Portability and Accountability Act (HIPAA) requirements that apply to this vendor relationship?

CYBERSECURITY ASKS

Is the vendor protecting our information, systems, and operations well enough for the access and risk involved?

A BAA MATTERS. IT IS NOT THE WHOLE SECURITY REVIEW.

HIPAA uses the term protected health information (PHI) for certain patient information. When a vendor handles PHI on your behalf, HIPAA often requires a Business Associate Agreement (BAA). A BAA creates important legal obligations, but it does not prove the vendor is secure.

WHEN IS A BAA USUALLY NEEDED?

Usually when a vendor creates, receives, stores, or sends PHI on behalf of your practice. Examples may include electronic health record, billing, cloud, managed IT, and some artificial intelligence vendors. If the relationship is unclear, pause before sharing protected patient information and involve your privacy or security lead, or legal counsel.

HOW TO READ THIS GUIDE

STRONG ANSWER

Signs that the vendor has a thoughtful approach and can explain how its protections work.

DIG DEEPER

Not automatically bad. The answer is incomplete, unclear, or needs proof. Ask follow-up questions.

RED FLAGS

Answers that should make you pause. Understand and resolve the concern before moving forward.

A red flag does not automatically mean "no." The goal is to understand the risk and make a deliberate decision.

1

What information and access do you need - and why?

STRONG ANSWER

- Clearly explains what information and systems are involved.
- Explains where the information goes and where it is stored or processed.
- Requests only the access needed to provide the service.

DIG DEEPER

- Says, "We may need access from time to time," without being specific.
- Understands the application but cannot explain how support staff access your systems or where the data goes.

RED FLAGS

- Requests broad electronic health record, network, database, or administrator access without a clear reason.
- Cannot explain what information it receives or where that information goes.

2

If a BAA is required, will you sign one? Do any other companies you use have access to our patient information?

STRONG ANSWER

- Will sign the BAA before receiving PHI when one is required.
- Clearly identifies other companies it uses that may handle your PHI.
- Explains how it makes sure those companies follow the privacy and security requirements that apply.

DIG DEEPER

- Will sign a BAA but is vague about other companies that may have access to your information.
- Says a parent company or cloud provider "handles that" without explaining how.

RED FLAGS

- Refuses a BAA even though the service requires the vendor to handle PHI on your behalf.
- Says, "We are HIPAA compliant, so a BAA is not necessary."

3

How do you control who can access our data and systems?

STRONG ANSWER

- Uses a separate account for each person.
- Gives people only the access their job requires.
- Quickly removes or changes access when someone leaves or changes roles.
- Uses multifactor authentication (MFA) - such as a password plus an app prompt, security key, or code - for remote access, systems reachable from the internet, and high-risk administrator accounts.
- Reviews administrator and service accounts regularly.

DIG DEEPER

- MFA exists but is optional or used on only a few important systems.
- Removing access depends mostly on someone remembering to do it.

RED FLAGS

- Shared administrator accounts are routine without a clear technical reason and other safeguards.
- Former team members or contractors can keep access.
- High-risk access relies on a password alone without a documented reason and other protections.

CURRENT LAW + GOOD PRACTICE

HIPAA today: HIPAA requires organizations to control access to electronic patient information and verify that users are who they claim to be.

Good cybersecurity practice: Use MFA for remote access, systems reachable from the internet, and administrator accounts. HHS lists MFA as a healthcare cybersecurity best practice.

Proposed change: HHS has proposed stronger MFA requirements in the HIPAA Security Rule. Those changes are not current law.

QUESTION 4

4

How do you protect the computers, servers, and other systems that store or access our information?

STRONG ANSWER

- Keeps systems and software supported and up to date.
- Uses secure settings instead of relying only on default configurations.
- Uses tools that can prevent or detect malicious software and suspicious activity.
- Protects sensitive information while it is being sent and while it is stored.
- Protects backups and other copies of sensitive information, not just the live system.

DIG DEEPER

- Security varies widely between systems.
- Important protections are available but not consistently turned on.
- The vendor cannot clearly explain which security settings it manages and which ones are your responsibility.

RED FLAGS

- Unsupported or unmanaged systems routinely access sensitive information without other safeguards that meaningfully reduce the risk.
- Systems that access customer data have little or no protection against malicious software or suspicious activity.
- Sensitive information is routinely stored or sent without reasonable protection and the vendor cannot explain why.

HIPAA TODAY

HIPAA today: Encryption is an addressable safeguard under the current HIPAA Security Rule. Addressable does not mean optional. The organization must decide what is reasonable and appropriate for the risk and document that decision.

5

How do you find and fix security weaknesses - including problems with older or connected medical devices?

STRONG ANSWER

- Keeps track of the system software, and devices used to provide the service.
- Watches for important security alerts and known vulnerabilities.
- Uses a repeatable process to find and prioritize weaknesses.
- Has a clear process for installing and verifying security updates.
- When an older system or medical device cannot be patched quickly, uses other protections such as separating it from the broader network, limiting what it can communicate with, controlling remote access, and monitoring it.
- Has a plan to replace or retire unsupported technology over time.

DIG DEEPER

- Updates are installed, but there is no clear process for deciding which vulnerabilities need attention first.
- Security scanning is irregular or covers only part of the environment.
- A device cannot be patched, but no one can clearly explain what other protections are reducing the risk.

RED FLAGS

- No repeatable process exists for finding and fixing vulnerabilities.
- Critical systems are running unsupported software with no meaningful safeguards around them.
- Vulnerable medical or connected devices sit on the same broad network as other systems with no deliberate isolation, access limits, or monitoring.
- "We patch when something breaks."

GOOD CYBERSECURITY PRACTICE

Good cybersecurity practice: HHS identifies attacks against network-connected medical devices as a healthcare cybersecurity threat. HHS also recommends protections such as separating higher-risk legacy systems from the broader network when appropriate. Stronger network-segmentation requirements have been proposed for HIPAA, but those proposed changes are not current law.

6

How do you protect your team from phishing, social engineering, and human error?

STRONG ANSWER

- Provides recurring cybersecurity training that matches people's roles.
- Uses email protections and MFA where appropriate.
- Makes it easy for people to report suspicious messages or activity.
- Teaches people how to protect sensitive information and credentials.
- Uses technical safeguards so security does not depend on people being perfect.

DIG DEEPER

- Training is treated mainly as a once-a-year checkbox.
- Email filtering exists, but people do not have a clear way to report suspicious messages.

RED FLAGS

- No cybersecurity awareness program exists for people with access to sensitive systems or information.
- The vendor treats phishing and social engineering as entirely the user's problem.

WHY THIS MATTERS

Why this matters: HHS identifies social engineering as a major healthcare threat and includes email security and basic cybersecurity training in its healthcare cybersecurity guidance.

7

How do you detect suspicious activity and figure out what happened?

STRONG ANSWER

- Records important activity in systems that handle sensitive information.
- Monitors for suspicious activity and has a clear process for escalating concerns.
- Uses security monitoring appropriate to the systems and services it protects.
- Can investigate who accessed a system, what changed, and what information may have been affected.

DIG DEEPER

- Logs exist, but they are rarely reviewed or are kept for too little time to support an investigation.
- Monitoring covers only part of the service.
- The vendor mainly relies on customers to notice when something is wrong.

RED FLAGS

- The vendor cannot reliably determine who accessed sensitive systems or what changed.
- Security incidents are usually discovered only after a customer reports a problem.

MED

QUESTION 8

8

If there is a security incident, how will you respond - and when will you tell us?

STRONG ANSWER

- Has a written incident-response plan and clearly assigned responsibilities.
- Can explain how it will contain the problem, investigate it, recover, communicate, and improve afterward.
- Has a clear customer-notification commitment in its contract.
- Shares useful information as it becomes known instead of waiting until every detail is final.
- Tests or practices its incident-response process.

DIG DEEPER

- Says, "We notify customers when required by law," but gives no practical notification timeframe.
- Has an incident plan but does not test or practice it.
- Cannot clearly explain who will communicate with you during an incident.

RED FLAGS

- Has no defined incident-response or customer-notification process.
- Will not commit to telling you about an incident that materially affects your data or service.

HIPAA BASELINE

HIPAA baseline: When a business associate discovers a breach of unsecured PHI, it must notify the covered entity without unreasonable delay and no later than 60 days after discovery. A contract can require faster notification.

9

If your systems fail or are attacked, how will you keep our practice operating and restore our data or service?

STRONG ANSWER

- Has written backup, recovery, and continuity procedures that fit the importance of the service.
- Protects backups from the same threats that could affect live systems.
- Can explain how quickly critical services should be restored and how much data could be lost.
- Regularly tests whether data or systems can actually be restored.
- Tracks problems found during testing and fixes them.
- Understands outside dependencies that could slow recovery.

DIG DEEPER

- Backups exist, but restore testing is irregular or undocumented.
- Recovery expectations are described only as "best effort."
- The vendor can say data is backed up but cannot explain when it was last restored successfully.

RED FLAGS

- The vendor cannot show that critical data or services are recoverable.
- The first meaningful restore test would happen during a real incident.
- Backups can be changed or deleted through the same access that could compromise the live systems.

10

What evidence can you provide that your security program is actually working?

STRONG ANSWER

- Provides objective evidence that fits the vendor's access, risk, and importance to your operations.
- Can show current security testing, risk assessments, recovery-test results, vulnerability-management records, or other reasonable evidence.
- For higher-risk services, may also provide independent assurance such as a SOC 2 Type 2 report (an independent report on security controls), HITRUST certification, ISO/IEC 27001 certification, or a comparable assessment.
- Can explain what the evidence covers, what it does not cover, and how important findings were fixed.

DIG DEEPER

- Provides only a self-completed questionnaire or marketing statement with little supporting evidence.
- Evidence is old or does not clearly cover the service you are buying.
- Points to a report or certification but cannot explain whether your service or environment is actually included.

RED FLAGS

- Refuses to provide any meaningful assurance for a high-risk service and offers no reasonable explanation or alternative evidence.
- Claims that HHS or the HHS Office for Civil Rights (OCR) has "HIPAA-certified" the company or technology.

IMPORTANT

Important: HIPAA does not require every business associate to give every customer an audit report, and HHS/OCR does not certify specific technology products. A practice may still ask for reasonable evidence based on the vendor's risk. A SOC 2 report is one possible form of evidence, not a requirement.

11

Will any of our information be processed by artificial intelligence or used to train or improve an AI system?

STRONG ANSWER

- Clearly explains whether artificial intelligence (AI) is used and why.
- Explains what information is sent to the AI system and which AI provider or other companies are involved.
- Explains how long the information is kept and whether it is used to train, fine-tune, test, or improve AI models or services.
- If PHI is involved, explains how the HIPAA business-associate relationship and required safeguards are handled.
- Gives you enough information to make a deliberate decision about the risk.

DIG DEEPER

- Says AI is used but cannot clearly explain what data is sent, where it goes, how long it is kept, or who else receives it.
- Buries statements such as “we may use data to improve our services” in general terms without explaining what that means for your information.

RED FLAGS

- PHI is sent to an AI service that the vendor cannot clearly identify or account for under the HIPAA relationship.
- The vendor cannot tell you whether your information is kept or used to train or improve AI models.

WHY ASK NOW

Why ask now: Current HHS guidance specifically includes a third-party AI chatbot handling patient PHI on behalf of a provider as an example of a business-associate relationship.

12

Who is responsible for security, and what happens to our data and access when the relationship ends?

STRONG ANSWER

- Clearly explains which important security responsibilities belong to the vendor, which belong to your practice, and which are shared.
- Reviews those responsibilities when the service starts and when it changes.
- Explains how your data can be exported when the relationship ends.
- Defines how data will be returned, retained, or destroyed.
- Removes vendor accounts, remote access, integrations, and other access paths when they are no longer needed.
- Explains how it will help with a safe transition to another vendor when appropriate.

DIG DEEPER

- Responsibilities are scattered across several documents or depend on assumptions.
- The vendor can delete live data but cannot clearly explain backup retention, export format, or how access is removed.

RED FLAGS

- Says, "We handle security," but cannot explain who owns important controls.
- Says, "HIPAA is the customer's problem," even though the vendor is a business associate handling PHI electronically.
- Your practice could lose access to needed information or leave vendor access active after the relationship ends.

IMPORTANT

Important: A healthcare practice and its business associates can both have HIPAA Security Rule responsibilities. Outsourcing a service does not remove the need to clearly define who is responsible for what.

What to do with the answers

1

ARE THE HIPAA REQUIREMENTS THAT APPLY BEING MET?

Where HIPAA applies, make sure the legal and contract requirements are covered.

2

IS THE CYBERSECURITY STRONG ENOUGH FOR THE ACTUAL RISK?

A control does not have to be explicitly named in HIPAA to be a sensible protection. Consider the data, access, threats, and importance of the service.

3

COULD A FAILURE INTERRUPT PATIENT CARE OR PRACTICE OPERATIONS?

A vendor can be critical even if it never handles PHI. Think about what an outage, compromise, stolen credential, or failed recovery would do to your practice.

IMPORTANT GUARDRAIL

This guide is not a pass/fail certification. Good answers do not automatically make a vendor secure, HIPAA compliant, or right for every practice. Use the answers to decide what needs more proof, stronger safeguards, contract changes, risk acceptance, or escalation.

Business Associate Agreement essentials

When a vendor is a HIPAA business associate, the Business Associate Agreement generally needs to address:

1. How PHI may and must be used or disclosed.
2. Limits on other uses or disclosures.
3. Appropriate safeguards, including the HIPAA Security Rule requirements that apply to electronic PHI.
4. Reporting of improper uses or disclosures, breaches of unsecured PHI, and security incidents when applicable.
5. Requiring subcontractors that handle PHI to follow the same applicable requirements.
6. Support for applicable patient rights, including access, amendment, and certain accounting requirements.
7. Making relevant records available to HHS for compliance purposes.
8. Returning or destroying PHI when the relationship ends, when feasible, and continuing to protect PHI that cannot be returned or destroyed.
9. The covered entity's right to end the agreement for a material violation.

OTHER CONTRACT ITEMS WORTH DEFINING CLEARLY

- Faster incident notification than HIPAA's outside deadline.
- Data export and transition help.
- Backup, restore, and continuity expectations.
- Recovery times and service availability.
- Where data may be stored or processed.
- Notice when important subcontractors or service providers change.
- Which security responsibilities belong to the vendor, the practice, or both.
- What security evidence is appropriate for the risk.
- How long data is kept and how it is deleted.



Keep the full version.

USE IT WITH ANY VENDOR.

Scan for the editable Vendor Cybersecurity & HIPAA Due-Diligence Questionnaire, the Business Associate Agreement (BAA) Essentials Reference, and current HHS/OCR cybersecurity and HIPAA sources.



INTUITIVE IT
385-312-1900
IntuitiveITS.com

marketing.IntuitiveITS.com/UMGMA-2026

Built to help healthcare practices ask better questions of any vendor - including us.

Tailored IT. Hardened Security. Connected Care.

Educational resource only. Not legal advice and not a HIPAA compliance certification. HIPAA obligations depend on the facts of the relationship. Cybersecurity protections should be selected and managed based on risk.

VERSION 2.3 - AUGUST 2026