HEALTHCARE COMPLIANCE GUIDE

Preparing for a HIPAA Security Risk Analysis

What to gather before your assessment begins, what the assessment covers, what findings to expect, and how remediation planning works.

For: Practice owners, administrators, and compliance leads **Edition:** November 2026

Web: spmadvisors.net

ABOUT SPM ADVISORS

Veteran-owned cybersecurity and digital forensics firm helping organizations, healthcare practices, and individuals understand their risk and respond when something goes wrong. Learn more at spmadvisors.net.

INSIDE THIS GUIDE

1. Preparation is not the risk analysis
2. Why this matters now
3. Preparation checklist
4. Assessment scope
5. How the assessment works
6. Expected findings
7. Remediation planning

Preparation is not the risk analysis

The HIPAA Security Rule requires covered entities and business associates to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic protected health information (ePHI) they hold (45 CFR 164.308(a)(1)(ii)(A)). This guide helps you get ready for that assessment. It is important to be clear about what preparation does and does not accomplish.

Preparation (this guide)

- Gathers the lists, documents, and contacts an assessor needs
- Identifies who should be interviewed
- Shortens the assessment and reduces back-and-forth
- Surfaces obvious gaps early
- **Does not** satisfy the risk analysis requirement on its own

The risk analysis

- Identifies where ePHI is created, received, maintained, and transmitted
- Identifies reasonably anticipated threats and vulnerabilities
- Evaluates current safeguards
- Rates the likelihood and impact of each risk and assigns a risk level
- Is documented, and is reviewed and updated as your environment changes

COMMON MISCONCEPTIONS

None of the following is a risk analysis by itself: a completed checklist, a signed policy binder, an EHR vendor's "HIPAA compliant" statement, a vulnerability scan, a penetration test, or a cyber insurance application. Each can be useful evidence. None replaces the documented, organization-wide assessment the rule requires.

Why this matters now

A missing or incomplete risk analysis remains one of the most frequently cited problems in HIPAA enforcement. The HHS Office for Civil Rights (OCR) continues to resolve investigations under its Risk Analysis Initiative, and "did you do the risk analysis?" is typically one of its first questions after a breach report or complaint.

- **The current Security Rule is fully in force.** HHS proposed significant Security Rule changes in January 2025. As of this guide's edition, those changes have not been finalized. Your obligations today are under the existing rule.
- **Risk management follows the analysis.** The rule also requires you to implement security measures that reduce identified risks to a reasonable and appropriate level (45 CFR 164.308(a)(1)(ii)(B)). An analysis with no follow-through leaves you exposed.
- **It is not a one-time project.** Update the analysis periodically and whenever you have significant changes, such as a new EHR, a new location, a merger, a move to cloud services, or a security incident.

Preparation checklist

Gather what you can. If something does not exist, note that; a missing document is itself useful information for the assessment.

1. Organization and people

- [ ] Organization chart and list of practice locations
- [ ] Workforce count, including part-time, remote, and contract staff
- [ ] Names of your designated Security Official and Privacy Official
- [ ] Job roles and the systems each role uses
- [ ] Remote work and personal device (BYOD) arrangements

2. Systems and technology

- [ ] EHR, practice management, billing, and patient portal systems
- [ ] Email, file sharing, cloud storage, and collaboration tools
- [ ] Telehealth, e-fax, texting, and patient messaging tools
- [ ] Laptops, desktops, tablets, and phones that access ePHI
- [ ] Network diagram, firewall, Wi-Fi, and remote access methods
- [ ] Backup systems and where backup copies are stored
- [ ] Connected medical devices, imaging, lab interfaces, copiers, and scanners

3. Information and data flows

- [ ] Where ePHI enters (intake, referrals, labs, portals, fax)
- [ ] Where it is stored, including exports, spreadsheets, and scanned paper
- [ ] Where it is sent (payers, labs, billing companies, other providers)
- [ ] Any ePHI kept on personal devices or personal email
- [ ] How data is disposed of when devices are retired

4. Vendors and business associates

- [ ] List of vendors that create, receive, maintain, or transmit ePHI
- [ ] Signed business associate agreements (BAAs) for each
- [ ] IT or managed service provider contract and scope of services
- [ ] Vendor security reports (for example, SOC 2) where available
- [ ] Vendors with remote access to your systems

5. Documents and records

- [ ] Prior risk analyses and remediation or risk management plans
- [ ] Security policies and procedures, with review dates
- [ ] Workforce security training records
- [ ] Encryption status of laptops, phones, and backups
- [ ] Contingency plan, backup test results, and disaster recovery plan

- [ ] Sanction policy and any applied sanctions
- [ ] Access review records and new-hire / termination procedures
- [ ] Device and software inventory
- [ ] Security incident and breach logs, including near misses
- [ ] Audit log settings and evidence of log review
- [ ] Cyber insurance policy and most recent application
- [ ] Physical security details: locks, alarms, visitor procedures

6. People to schedule

- [ ] Practice owner or administrator, and the Security Official
- [ ] IT provider or internal IT lead, and the EHR administrator
- [ ] Representatives from front desk, clinical, and billing staff, who often know how work actually gets done

Assessment scope

The risk analysis must cover **all** ePHI your organization creates, receives, maintains, or transmits, in every location and on every system or device, including what your vendors handle on your behalf. Scope is where many analyses fall short.

Scope at a glance

CLEARLY IN SCOPE	IN SCOPE, BUT OFTEN MISSED	DISCUSS WITH YOUR ASSESSOR
• EHR and practice management • Workstations and servers • Email and patient messaging • Backups	• Personal phones used for work • Old laptops and retired drives • Copiers and multifunction printers • Accounts for former staff • Shared spreadsheets and exports	• Paper records (covered by the Privacy Rule; often reviewed together) • Affiliated entities or shared networks • Planned systems not yet live

How the assessment works

1. **Kickoff.** Confirm scope, contacts, timeline, and how documents will be shared securely.
2. **Document review.** The assessor reviews what you gathered and notes gaps.
3. **Interviews and walkthroughs.** Conversations with staff and a review of how ePHI actually moves through the practice.
4. **Technical validation.** Spot checks of configurations such as multi-factor authentication, encryption, patching, backups, and user access.
5. **Risk rating.** Each threat and vulnerability is rated for likelihood and impact to produce a risk level.
6. **Report and risk register.** A documented analysis with findings ranked by risk, ready to drive remediation.

Expected findings

Findings are normal. Nearly every assessment produces them, and a well-documented list of findings with a plan to address them is far stronger than a clean report nobody believes. Common examples include:

- Multi-factor authentication missing on email, remote access, or admin accounts
- Incomplete inventory of devices, software, or vendors
- Missing or outdated business associate agreements
- Laptops, phones, or backups without encryption
- Shared logins or generic accounts
- Backups that are not isolated or have never been test-restored
- Accounts for former staff still active
- Audit logs enabled but never reviewed
- Policies that do not match day-to-day practice
- Training that is irregular or undocumented

Remediation planning

The analysis tells you where you stand. The risk management plan records what you will do about it. A practical plan:

- **Prioritizes by risk level,** addressing high risks first while picking up quick, low-cost fixes along the way.
- **Assigns a named owner, a target date, and an estimated cost** to each item.
- **Documents accepted risks.** If you decide not to address a risk, or to address it differently, record the reasoning and who approved it. Some Security Rule specifications are "addressable," which means you must assess them and document your decision, not that they are optional.
- **Tracks progress** and is reviewed regularly by leadership.
- **Feeds the next analysis,** so each cycle starts from an accurate picture.

Example risk management plan entries

FINDING	RISK LEVEL	ACTION	OWNER	TARGET
No MFA on remote access to EHR	High	Enable MFA for all remote users	IT provider	30 days
Two vendors without signed BAAs	Medium	Execute BAAs or stop sharing ePHI	Practice administrator	45 days
Backups never test-restored	High	Perform and document a restore test	IT provider	30 days

KEEP THE RECORD

HIPAA requires that Security Rule documentation, including your risk analysis and the decisions that follow it, be retained for six years from the date of creation or the date it was last in effect, whichever is later. Keep each version, not just the latest.

BEFORE YOUR ASSESSMENT

You do not need everything on the checklist to begin. Start with your system list, vendor list, and any prior analysis. A good assessor will help you fill in the rest, and the gaps you find along the way become part of the plan.

This guide provides general information for planning purposes. It is not legal advice and does not create a client relationship. Requirements and product features change; confirm current details before relying on them. © 2026 SPM Advisors LLC. Edition: November 2026.