ePHIJournal
an ePHIShield publication www.ephishield.com

HIPAA Compliance for Independent Practices

Live Breach Tracker ↗

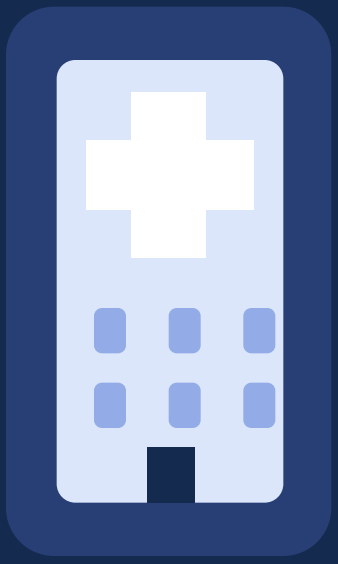
FREE INAUGURAL EDITION

NOVEMBER 2026 / VOL. 01

THE INDEPENDENT PRACTICE ISSUE

The Fight to Remain Independent

Rising costs. Proposed HIPAA changes. Practical first steps for smaller practices.



INSIDE Proposed Rule / Risk Analysis / Training / Breach Alert

Practical HIPAA intelligence for independent medical practices.

Source-grounded reporting, real OCR cases, and manageable action steps—written for people who must protect patient information while running a practice.

WELCOME

A Useful Starting Point

An introductory issue for independent practices navigating HIPAA today—and evaluating the changes HHS has proposed.

From the editor

Independent practices deliver something that large systems cannot always replicate: continuity, local accountability and a personal relationship between physician and patient. But preserving that independence requires managing costs, technology and compliance responsibilities that compete with time for patient care.

This inaugural issue focuses on decisions an office manager or physician can actually make. You will find an evidence-based explanation of the proposed HIPAA Security Rule, a practical distinction between an IT security scan and a regulatory risk analysis, real enforcement and breach cases, and a checklist for evaluating your own program.

The editorial standard is simple: **What is required? Why does it matter to a smaller practice? What should the practice do next?** We believe responsible urgency comes from facts, not fear.

Inside this edition

- 03–04 The Fight to Remain Independent
- 05–06 The Proposed HIPAA Security Rule
- 07 Today's Requirements vs. What Is Proposed
- 08–09 An IT Scan Is Not a Complete Risk Analysis
- 10 HIPAA Workforce Training That Matters
- 11 Breach Alert: Wichita Family Dental
- 12 Enforcement Watch: Shen Smiles
- 13–14 Ten-Question Practice Readiness Check
- 15 Your First 90 Days: A Practical Plan
- 16 Resources, Sources and Next Steps

REGULATORY STATUS | PROPOSED — NOT CURRENT LAW

HHS PLANNED FINAL ACTION: JULY 2027

Current HIPAA rules remain in effect. Check the live HHS agenda and Federal Register for changes before relying on the NPRM details in this dated issue.

View official HHS agenda

LEAD FEATURE / PART 1

The Fight to Remain Independent

How reimbursement, administrative pressure and the proposed Security Rule are changing the economics of smaller medical practices.

60.1% 2012 **42.2%** 2024

Share of physicians working in private practice (AMA)

For generations, independent medical practices have allowed physicians to build personal relationships with patients, exercise clinical judgment and remain connected to the communities they serve. But the business of remaining independent is becoming more difficult.

A changing practice landscape

According to the American Medical Association, the share of physicians working in private practice declined from **60.1% in 2012 to 42.2% in 2024**. That is a decrease of nearly 18 percentage points in 12 years—not a claim that 18% of practices closed, but a striking shift in where physicians work.

The AMA surveyed physicians whose private practices had been acquired and asked which factors mattered to the sale. Better negotiating power with payers was important or very important to **70.8%**; access to costly resources to **64.9%**; and managing payers' administrative and regulatory requirements to **63.6%**. These statistics are about broader business pressures, not specifically HIPAA.

Where HIPAA fits

HIPAA is one component of an accumulating administrative burden. A hospital network may have dedicated information security personnel, a privacy office, legal counsel and project managers. In a ten-person physician office, the same office manager may handle billing, scheduling, staffing, patient complaints, vendors and security paperwork.

The obligations do not disappear because the practice is small. And when responsibility is fragmented among the physician, an IT vendor and an office manager, the most dangerous question can be the simplest one: **Who is actually making sure our HIPAA requirements are being met?**

More than an IT expense

Compliance is sometimes treated as a software purchase or an annual training certificate. In reality, the Security Rule requires a continuing program of identifying risks, implementing safeguards, evaluating effectiveness and documenting decisions. Good software helps; it cannot replace management responsibility.

The financial challenge is therefore not just equipment and subscriptions. It is the time required to understand the practice's environment, organize evidence, train staff and follow through on corrective work.

AMA AMA25

LEAD FEATURE / PART 2

A Manageable Path Forward

The most important first step is an accurate understanding of where your practice stands.

What is required today

The HIPAA Security Rule already requires an **accurate and thorough risk analysis** of potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information (ePHI). It also requires risk management and a security awareness and training program. These are not obligations reserved for hospitals.

An EHR vendor's assurances, a vulnerability scan or a purchased policy binder may be useful components, but none automatically establishes that the practice has evaluated all of its ePHI risks. The practice must understand the scope of its own systems and vendors.

What could change next

HHS published proposed Security Rule amendments in January 2025. Among the proposals are more detailed written risk analyses; updates at least every 12 months; role-specific annual security awareness training; annual compliance audits; inventories and network maps; and more explicit technical safeguards and testing. **The changes are proposed, not binding law.** The agency's Unified Agenda lists **final action planned for July 2027**.

The proposal may change before finalization. But waiting for a final rule does not solve existing gaps. Practices with an incomplete risk analysis or undocumented training already have work to do under today's rules.

The answer is not an overnight overhaul

The workable starting point is to understand the current environment. A thorough SRA can identify where ePHI is handled, which risks are most significant and which safeguards need attention. Training can help personnel recognize threats and understand their responsibilities. Together, these can form a foundation for a prioritized risk-management plan—not a substitute for the other safeguards already required.

Five first steps

- **Establish your baseline.** Determine whether your existing SRA reflects today's systems, workflows, vendors and threats.
- **Identify and prioritize deficiencies.** Address urgent risks and document a reasonable corrective-action plan.
- **Train your workforce.** Cover relevant HIPAA responsibilities, provide practice-specific instruction and retain evidence.
- **Assign ownership.** Name who will coordinate the work, review completion and elevate unresolved risks.
- **Review and improve.** Revisit risks after incidents, technology changes and changes in practice operations.

You do not have to solve every problem today. But you do need to know where you stand—and begin addressing the problems that matter.

RULE SRA NPRM AGENDA

REGULATORY OUTLOOK / PART 1

The Proposed Security Rule

What independent practices need to know now: risk analysis, inventories and workforce training.

PROPOSED — NOT CURRENT LAW | HHS PLANNED FINAL ACTION: JULY 2027

The January 2025 HIPAA Security Rule proposal would make many cybersecurity expectations more explicit, documented and recurring. For small practices, the question is how to prepare responsibly without treating proposals as current law.

1. Risk analysis: a more detailed record

Today, the Security Rule requires an accurate and thorough analysis of risks to ePHI. The law does not prescribe one universal annual interval for an entirely new SRA. An analysis must remain accurate as the environment changes. OCR's guidance describes risk analysis as the first step in a continuing management process.

The NPRM proposes a more specific written assessment addressing technology inventories, network maps, reasonably anticipated threats, vulnerabilities, likelihood and risk levels. It also proposes review, verification and updating **at least every 12 months** and when relevant changes occur. That is a recurring review obligation—not necessarily a requirement to buy a brand-new assessment each year.

2. Technology inventory and network map

ePHI does not reside only in the EHR. It may pass through desktops, laptops, billing portals, backup systems, document scanners, secure messaging systems and cloud vendors. The NPRM would require a documented inventory and network map showing relevant systems and ePHI movement, maintained on an ongoing basis and reviewed at least annually.

An office manager can begin by asking for a list of systems and vendors that create, receive, maintain or transmit ePHI, who administers them, where backups live and when access was last reviewed.

3. Security awareness training

The current Security Rule requires a workforce security awareness and training program, including management, but no universal annual frequency. Separately, the Privacy Rule requires appropriate workforce training on privacy policies and procedures, including training on relevant policy changes.

The proposed Security Rule would require security awareness training generally **at least once every 12 months**, based on workforce role, with additional timing and change-related requirements. Course completion alone cannot substitute for the practice's own procedures and responsibilities.

Why this deserves attention now

These proposals do not impose a current compliance deadline. They do, however, reveal the level of documentation, coordination and evidence HHS was considering. Practices that cannot identify their systems, document risks or demonstrate training have an actionable starting point today.

NPRM FR RULE

REGULATORY OUTLOOK / PART 2

How the Proposals Could Change Operations

Audits, technical safeguards and incident response could become more explicitly prescribed.

PROPOSED — NOT CURRENT LAW | HHS PLANNED FINAL ACTION: JULY 2027

4. Annual compliance audits

The current Security Rule requires periodic technical and nontechnical evaluations. The NPRM would add a documented **Security Rule compliance audit at least every 12 months**. This is different from an SRA: a risk analysis studies threats and vulnerabilities to ePHI; a compliance audit tests conformity with applicable regulatory requirements.

5. Technical safeguards and testing

The proposal would generally remove the distinction between required and addressable implementation specifications, subject to limited exceptions. It would also make more explicit demands involving multifactor authentication, encryption of ePHI at rest and in transit, network segmentation, configuration controls, vulnerability scanning at least every six months and penetration testing at least annually.

Under today's Rule, an "addressable" specification is not optional. The practice must evaluate it and either implement it or document an appropriate permitted alternative. The future rule could narrow those choices, but no one should describe those proposed specifics as currently mandatory merely because they appear in the NPRM.

6. Incident response and recovery

Current rules already require security incident procedures and contingency planning. The proposal would add more prescribed written procedures, testing and restoration expectations, including restoration of certain critical systems and data within 72 hours following specified loss events.

A physician office should already know whom to call if its EHR becomes unavailable, how to preserve evidence, how downtime care proceeds, what backups are available and who assesses notification obligations. Those questions matter whether the rule is amended or not.

A realistic plan for a small practice

- Review the last documented SRA against the practice's actual technology and workflows.
- Inventory systems and vendors that handle ePHI; ask who owns access controls, backup testing and log review.
- Establish an appropriate workforce training and documentation process.
- Separate gaps under current law from possible future changes, then prioritize existing obligations first.

The **HHS Unified Agenda lists final action planned for July 2027**. A final rule could differ materially from the proposal and carry future compliance dates. Preparation should be based on verified present requirements and prudent operational improvements, not an invented countdown.

NPRM FR AGENDA

KEEP THIS PAGE

HIPAA: Today vs. Proposed

A quick reference for the office manager and physician owner.

PROPOSED — NOT CURRENT LAW | HHS PLANNED FINAL ACTION: JULY 2027

AREA	CURRENT SECURITY RULE	2025 NPRM PROPOSES
Risk analysis	Accurate, thorough analysis required; ongoing updates as warranted. No universal annual interval.	Written detail; review, verify and update at least every 12 months.
Security training	Workforce security awareness and training required; no universal annual frequency.	Role-specific security awareness training at least every 12 months.
Compliance review	Periodic technical and nontechnical evaluations required.	Documented Security Rule compliance audit at least annually.
Asset inventory	Scope must cover ePHI and risks; no prescribed inventory/map format.	Technology inventory and network map, updated at least annually.
Encryption and MFA	Access safeguards required; some encryption specs addressable (not optional).	More explicit encryption and MFA requirements, limited exceptions.
Technical testing	Identify and manage risks; no fixed 6-month scanning or annual pen-test rule.	Vulnerability scanning at least 6-monthly; pen-testing at least annually.
Incident response	Security incidents and contingency plans must be addressed.	More detailed plans, testing, and specified 72-hour restoration procedures.
Business associates	BA agreements and appropriate safeguards already required.	Additional written annual verification of certain BA safeguards.
Documentation	Required policies, procedures and records retained and reviewed.	More written records; most addressable specs would become required.

Bottom line: The NPRM does not replace current law. Begin with an accurate SRA, required safeguards and appropriate training; monitor the official rulemaking before treating any proposed duty as a compliance deadline.

RULE PRIV NPRM AGENDA

SECURITY RISK ANALYSIS / PART 1

Your IT Company Runs Scans. Is That a HIPAA Risk Analysis?

A technical vulnerability scan and a regulatory risk analysis are useful—but different—tools.

A clean vulnerability report can be valuable—but it does not automatically satisfy HIPAA's requirement for a comprehensive Security Risk Analysis (SRA). Here is why the distinction matters.

Two different questions

A technical scan asks whether particular software, devices or networks exhibit detectable weaknesses: an outdated application, an exposed service, a missing patch or a misconfiguration. Its output is usually a list of technical findings and possible fixes.

A HIPAA risk analysis asks a broader management question: what reasonably anticipated threats and vulnerabilities could affect the confidentiality, integrity or availability of **all** the ePHI the organization creates, receives, maintains or transmits? Its scope includes not only technical assets but also personnel, procedures, vendors, physical locations, backups and operations.

Where ePHI actually travels

Consider a two-physician office. Patient data may be stored in its cloud EHR, sent to a laboratory, viewed from a billing workstation, exported for a referral, included in patient emails or backed up by a managed services provider. The scanner used by its IT company may not see each of those processes, contractual relationships or physical safeguards.

A sound SRA records where ePHI exists and moves, what can go wrong, the safeguards already present, the likelihood and impact of plausible events, and the residual risks that remain. Its exact method can vary with practice size and complexity; OCR does not mandate a single proprietary scoring model.

The evidence behind the judgment

A useful assessment is not merely a spreadsheet marked "compliant." It should be supported by interviews, system and vendor inventories, documented observations, policy review, available configuration evidence and decisions about risk. When a conclusion depends on the office manager's assertion or a vendor's representation, that limitation should be visible.

SRA RULE

The purpose is not to collect the largest possible binder. It is to enable decisions the physician and office manager can understand, defend and follow through on.

SECURITY RISK ANALYSIS / PART 2

What a Real SRA Should Give You

Evidence, decisions, priorities and a clear path to risk management.

Risk analysis is not risk management

A risk analysis identifies and evaluates risks. Risk management is the distinct obligation to implement security measures sufficient to reduce those risks to a reasonable and appropriate level. Finding a risk is not the same as addressing it. A credible SRA should therefore produce a usable route into corrective action.

The questions to ask an IT vendor

- **Scope:** Does the work cover every location, information system and vendor that handles ePHI—or only the local network?
- **Threats:** Are human error, inappropriate access, downtime, physical loss and third-party issues evaluated alongside malware?
- **Risk method:** Are likelihood and impact explained and documented, rather than replaced by a generic pass/fail score?
- **Evidence:** Which findings were observed, supported by records or reported by personnel?
- **Follow-through:** Does the practice receive a prioritized remediation list and a way to monitor progress?

What a usable SRA deliverable looks like

A practical report should identify scope and assumptions, describe the practice's ePHI environment, document material threats and vulnerabilities, characterize risk, summarize existing safeguards, and identify corrective priorities. It should also make ownership and follow-up responsibilities clear without claiming that the report itself makes the practice fully compliant.

A small office can begin today by locating its most recent SRA, asking who approved it, checking whether it includes the current EHR and vendors, and comparing its findings with actual remediation records. If the practice cannot produce those materials, that is a reason to investigate—not automatically proof of a HIPAA violation.

A measured first step

An accurate, comprehensive baseline is the foundation for future updates and better spending decisions. It prevents the practice from treating every technology purchase as equally urgent and directs effort toward risks that matter most.

Takeaway: Ask whether the document in your file is a technical scan, a broader risk analysis, or both. Know which responsibility it actually fulfills.

SRA RULE FR

WORKFORCE EDUCATION

HIPAA Training That Changes Behavior

Beyond a completion certificate: practical instruction for the entire practice.

HIPAA training should change how people act at work—not simply generate certificates. For a small practice, a repeatable program can be one of the most affordable ways to reduce avoidable mistakes.

There is more than one HIPAA training duty

The Privacy Rule requires covered entities to train workforce members on relevant policies and procedures as necessary and appropriate for their functions, and to document that training. The Security Rule separately requires a security awareness and training program for all workforce members, including management.

Neither current provision imposes a universal annual training schedule on every practice in precisely the way proposed in the 2025 NPRM. Annual refreshers can be good practice, while changes in duties, systems, policies, or incidents may call for additional instruction sooner.

Focus on ordinary workday decisions

- Front-desk staff should know how to authenticate a caller and handle a patient-record request.
- Clinical staff should know when access to a chart is permitted and what to do after a suspicious email.
- Office managers should know where training records are kept, who reports incidents and when policies need updating.
- New personnel should receive instruction appropriate to their role, not simply inherit assumptions from coworkers.

What OCR's Ambry case illustrates

In September 2026, OCR announced a **$700,000 settlement** with Ambry Genetics over potential HIPAA Security Rule violations following a phishing-related incident discovered in 2020. OCR's corrective-action terms included risk analysis, risk management, access controls and workforce training. This was a negotiated settlement of potential violations, not a court judgment that a phishing click alone established liability.

The practical lesson is that incident prevention and organizational security governance belong together. Teach employees to recognize suspicious requests; also maintain meaningful access procedures, authentication controls and response processes.

Training you can demonstrate

Keep records of who was trained, when, on which topics, and any necessary practice-specific instruction. Follow up when staff members do not understand a critical procedure. Standardized HIPAA courses are useful foundations, but they cannot by themselves replace training on the practice's own systems, policies and roles.

RULE PRIV AMBRY

REAL-WORLD CASE STUDY

One Employee Email Account. 1,273 People Affected.

Wichita Family Dental, Kansas | Reported to HHS on September 11, 2026

! BREACH ALERT / SMALL-PRACTICE CASE

Wichita Family Dental, a Kansas dental practice, reported an email-related hacking/IT incident affecting **1,273 individuals** to HHS OCR on September 11, 2026. The record offers a concrete opportunity for practices to examine everyday email safeguards.

What has been publicly reported

According to the public OCR breach listing, the incident was categorized as a hacking/IT event involving email. Trade reporting citing the practice's notice says an employee email account was accessed without authorization, discovered in May 2026, and that certain messages were accessed. Reported potentially affected information included identifying, financial and dental-record details; exposure may vary from person to person.

A report to OCR is not, by itself, an OCR finding that the practice violated HIPAA. The public information available here also does not establish the precise attack technique or whether any particular safeguard was absent. We should resist jumping from "breach" to unsupported allegations of negligence.

What a small office can examine

- Are strong authentication controls in place for employee email and remote access?
- Do staff know how to report a suspected compromised account immediately and to whom?
- Does the SRA consider email, attachments, retention, exports and ePHI-sharing workflows?
- Can the practice quickly determine which accounts and records were exposed if an incident occurs?

The larger perspective

Some incidents affect relatively few people compared with national headline breaches, yet still create patient-notification, investigation, documentation and operational work. The business lesson is to prepare response procedures before an incident, rather than invent them after discovery.

THE BREACHES OUTSIDE THE PUBLIC LIST

74,299
Fewer than 500 individuals

663
500 or more individuals

HHS documented these reported breach incidents for calendar year 2024. Smaller reportable breaches are reported to OCR under a different timetable and do not appear in the public 500-plus list. These are historical counts of incidents, not live totals or exclusively hacking events.

HHS 2024 report and reporting guidance Case record: OCR Local reporting

ENFORCEMENT WATCH

A Records Request. A $140,000 Settlement.

OCR's 56th Right of Access enforcement action offers a practical privacy lesson.

A request for patient records is routine office work. But an alleged failure to provide access can lead to an OCR investigation that examines a practice's underlying HIPAA procedures.

The Shen Smiles case

On October 8, 2026, HHS OCR announced its **56th Right of Access enforcement action**, a **$140,000 settlement** involving Pennsylvania dental practice Shen Smiles. The matter arose from a complaint alleging failure to provide timely access to protected health information. OCR also identified potential deficiencies concerning Privacy Rule and Breach Notification Rule policies and procedures.

The case was resolved by agreement. It is important to distinguish potential violations resolved in a settlement from findings established after litigation. The enforcement announcement also references an assertion involving stolen records; that should not be transformed into a confirmed, separately adjudicated breach.

Know the response clock

Under the HIPAA Privacy Rule, covered entities generally must act on an individual's access request within **30 calendar days**. One additional 30-day extension may be available if the entity gives the required written notice within the initial period. These are outer limits, not suggested waiting periods; many requests should be completed sooner.

A practical access-request workflow

- Record the request date, identity-verification steps and the records requested.
- Assign a responsible person and track the deadline, even if an EHR vendor helps fulfill the request.
- Use written, tested procedures for the requested form and format, permitted fees and any lawful denial.
- Document what was provided and when, and provide a compliant extension notice when justified.

The takeaway: HIPAA compliance is not only cybersecurity. A practice also needs reliable processes for patient rights, privacy administration and workforce responsibilities. Training and written procedures should make those processes routine.

SHEN ACCESS PRIV

PRACTICE READINESS / PART 1

Ten Questions to Ask Your Practice

A self-review for the office manager and physician owner. Questions identify what to investigate; they are not a HIPAA compliance certification.

01 **Can we produce a current, comprehensive Security Risk Analysis?**

Find the last report and confirm scope, methodology, date, systems, locations, vendors and follow-up owners. A scan alone may not cover all ePHI risks.

STATUS: ☐ Yes ☐ No ☐ Unsure OWNER / EVIDENCE: _____

02 **Do we know every place ePHI is handled?**

Include the EHR, billing, email, cloud storage, referrals, laboratories, paper-to-digital workflow, remote devices and backup vendors.

STATUS: ☐ Yes ☐ No ☐ Unsure OWNER / EVIDENCE: _____

03 **Are identified risks being managed?**

Look for an active corrective-action log, risk owners, priorities, decisions and evidence that urgent issues are addressed.

STATUS: ☐ Yes ☐ No ☐ Unsure OWNER / EVIDENCE: _____

04 **Can we document workforce instruction?**

Identify new-hire, job-specific and refresher training. Retain completion records and evidence of instruction on local policies.

STATUS: ☐ Yes ☐ No ☐ Unsure OWNER / EVIDENCE: _____

05 **Do we know who is responsible for security and privacy?**

Confirm designated officials, reporting channels, escalation authority and who supervises vendor-related responsibilities.

STATUS: ☐ Yes ☐ No ☐ Unsure OWNER / EVIDENCE: _____

Use this checklist in a 20-minute management discussion. Note who will gather each answer, where the supporting record lives and when to revisit unresolved questions.

PRACTICE READINESS / PART 2

Five More Questions Worth Answering

A self-review for the office manager and physician owner. Questions identify what to investigate; they are not a HIPAA compliance certification.

06 Are user accounts and access reviewed?

Check role-based access, unique accounts, departures, password resets, remote access, audit logs and shared credentials.

STATUS: ☐ Yes ☐ No ☐ Unsure OWNER / EVIDENCE: _____

07 Could we continue patient care during a technology outage?

Know the downtime process, essential contacts, backup availability, recovery priorities and how restored data are verified.

STATUS: ☐ Yes ☐ No ☐ Unsure OWNER / EVIDENCE: _____

08 Do we know our vendor obligations?

Review business associate arrangements, EHR hosting, backup responsibility, subcontractor access and the method for reporting vendor incidents.

STATUS: ☐ Yes ☐ No ☐ Unsure OWNER / EVIDENCE: _____

09 Could we document a suspected breach response?

Confirm workforce reporting, triage, evidence preservation, required assessments, notification decisions and recordkeeping.

STATUS: ☐ Yes ☐ No ☐ Unsure OWNER / EVIDENCE: _____

10 Do we respond promptly to patient records requests?

Track requests, verification, 30-day clock, extensions, delivery and documentation. Privacy obligations deserve the same rigor as cybersecurity.

STATUS: ☐ Yes ☐ No ☐ Unsure OWNER / EVIDENCE: _____

How to interpret your answers: “I’m not sure” is a reason to gather evidence. “No” may indicate a gap needing review; it does not by itself prove a violation. Prioritize current legal obligations and urgent security risks first.

PRACTICAL ACTION PLAN

Your First 90 Days Toward Stronger Compliance

Not a promise of “100% compliance”—a structured beginning for a resource-constrained practice.

A first 90-day plan should not promise complete HIPAA compliance. Its value is turning uncertainty into accountable work while addressing urgent risks promptly.

Days 1–15 | Establish ownership and collect evidence

Name a coordinator for security and privacy work, confirm the designated Security Official and privacy contact, and locate the most recent SRA, risk-management plan, training records, policies, vendor agreements, incident-response steps, and contingency documentation. Record missing items rather than guessing. Escalate active security problems immediately; do not wait for day 90.

Days 16–30 | Understand the actual environment

Inventory systems, services and locations where ePHI is created, received, maintained or transmitted. Include EHR access, email, billing, referrals, laboratories, cloud providers and backups. Review whether the current SRA covers the real environment; if not, arrange for a comprehensive update.

Days 31–60 | Prioritize and begin corrections

Use the risk analysis to evaluate threats, vulnerabilities and existing controls. Address higher-risk deficiencies first, such as exposed accounts, poorly controlled remote access, untested backups or missing incident escalation. Assign owners and realistic due dates. Document interim safeguards when a permanent correction requires more time.

Days 61–90 | Train, test and document progress

Provide or refresh role-appropriate Privacy and Security Rule instruction, including practice-specific procedures. Conduct a short response tabletop: if the EHR or email becomes unavailable, who does what? Check whether staff can find the incident contact list, report a suspicious message and identify access-request deadlines.

After day 90 | Maintain the cycle

Schedule management reviews of open risks and changes in vendors, technology and workflows. Monitor OCR regulatory developments, including the 2025 Security Rule proposal. Preparation is worthwhile, but do not treat proposed provisions as law before a final rule supplies the actual requirements and compliance dates.

An independent practice does not need to become a hospital system. It does need an organized, documented process for knowing its risks and steadily improving safeguards.

SRA RULE NPRM

REFERENCE DESK

Keep Learning. Keep Improving.

Essential sources, practical resources and ways to follow developments.

SOURCES & REFERENCE MATERIALS

AMA Physician Practice Benchmark Survey

HHS OCR guidance on risk analysis

45 CFR 164.308 - Current administrative safeguards

45 CFR 164.530 - Privacy Rule workforce training

HHS OCR NPRM fact sheet

Federal Register, 90 FR 898, Jan. 6, 2025

HHS Unified Agenda, RIN 0945-AA22

HHS Annual Report to Congress on Breaches, 2024

HHS breach reporting requirements

HHS OCR large-breach listing

HHS OCR, Ambry Genetics settlement, Sept. 17, 2026

HHS OCR, Shen Smiles settlement, Oct. 8, 2026

HHS guidance on patient access deadlines

Becker's Dental Review: Wichita Family Dental

FREE ePHIJOURNAL SUBSCRIPTION

Receive future issues and source-verified regulatory alerts for independent practices. Our signup page is being developed; check the journal page for availability. You can read this edition without subscribing.

Visit the ePHIJournal page

OTHER ePHISHIELD RESOURCES

HIPAA Training

Security Risk Analysis & Services

Live Breach Tracker

Editorial and regulatory information checked November 3, 2026. This publication provides general education and does not constitute legal advice or a practice-specific compliance determination. Proposed requirements may change before any final rule.