A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY MAGAZINE

OCTOBER 2026



KAMEELAH SPENCE, MS, CHC, CCEP
DIRECTOR OF COMPLIANCE AT
RHA HEALTH SERVICES LLC

THINKING LIKE AN EVALUATOR (P6)

Beyond the paper program: Navigating the "prevent and detect" mandate (P12)

The future of healthcare compensation valuation: AI-enabled, expert-led (P20)

AI, life sciences compliance, and the future of monitoring and investigations (P26)

HCCA®

Reprinted with permission. Copyright © 2026 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA).



THE HIPAA DOCUMENTATION GAP CATCHING SMALL PRACTICES OFF GUARD

by Jose Noriega



Jose Noriega
(jnoriega@gradientdata.com) is the Founder and CEO of Gradient Data Solutions in Miami, FL.

I have helped several small practices pass HIPAA audits and cyber insurance renewals over the past 10 years. I am not a healthcare attorney or a U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) insider. I run the IT and compliance operations behind the scenes, the part most practices do not see until their auditor asks for it. What I have learned is that the hardest part of HIPAA is not actually doing the work; it is proving you did it.

A practice administrator called me last month. Her cyber insurance renewal had landed on her desk Friday afternoon with a response deadline for the following Wednesday. The questionnaire was 34 pages. She told me, almost apologetically, that her practice was actually doing most of the things being asked about. Staff training, access reviews, backup tests, but she had no way to prove it. The documentation was somewhere, scattered across email threads, a shared drive, and her predecessor's old notebook. She spent three weeks pulling records. The renewal came in on time, but at a higher premium, because three of the controls she was actually performing got marked "unable to verify."

I have had some version of this conversation with practice administrators a dozen times this year. The work is getting done. What is missing is the proof of it.

Why intent does not save you

Most small practices are solving for whether they are compliant. The test they are actually failing is whether they can prove it.

OCR does not audit intent. The HIPAA Security Rule requires covered entities to implement policies and procedures and, critically, to "maintain the policies and procedures implemented to comply with this

Reprinted with permission. Copyright © 2026 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA).

subpart in written (which may be electronic) form."[1] The regulation is explicit that documentation must be retained for six years from the date of its creation or the date when it last was in effect, whichever is later.[2]

When a breach notification triggers an investigation, the question is not, "Were you trying to protect protected health information (PHI)?" It is, "Show me your policies, your training logs, your access reviews, your risk assessment, your business associate agreements (BAAs), and your incident response plan. Dated. Signed. Current."

What auditors actually ask for

A practice that has done everything right but cannot assemble those records under time pressure is operationally the same as a practice that did not do the work. This is the gap that catches small practices off guard, and it usually has nothing to do with negligence or ignorance. It is paperwork that exists in theory but cannot be produced on demand.

OCR's published enforcement history reinforces the point. In recent resolution agreements involving small providers, the deficiency most frequently cited is rarely a missing technical safeguard. It is the absence of documentation proving that a required activity was performed.[3] A practice that ran staff training but cannot show completion logs is, for enforcement purposes, in the same position as a practice that skipped training entirely.

The same pattern shows up on cyber insurance renewal questionnaires. Carriers increasingly require documented evidence of controls before binding coverage. An unsigned policy, an undated training record, or an informal incident log often gets marked as a control failure even when the underlying activity occurred. That control failure translates directly into higher premiums, narrower coverage, or declined renewal.

The six-step documentation system

Here is the approach I have built for the practices I work with. None of it requires additional headcount. It does require deciding, once, that compliance documentation will be treated as a running log, not a one-time project. What follows is the exact sequence we implement when a practice comes to us with a documentation gap.

1. Define the artifact list, then automate production

The list of documents OCR and cyber insurers actually ask for is finite. Policies and procedures. Risk assessment. Workforce training logs. Access control reviews. BAAs with every vendor touching PHI. Backup test results. Incident response plan. Breach notification plan. Audit logs for PHI access. That is the core.

Know exactly what has to exist, then decide where each artifact lives and how it gets refreshed. The HHS Security Risk Assessment Tool, published jointly by the Office of the National Coordinator and OCR, is a practical starting point for the risk assessment itself.[4] For the rest of the artifact list, the goal is not to adopt a new tool but to make a deliberate choice about which tool already in use will hold each artifact.

2. Pick one system of record, and actually use it

Most small practices have pieces of compliance scattered across three places: email, a shared drive, and someone's head. The single biggest improvement here is not buying a new platform but deciding which one is the source of truth and moving everything else into it.

It could be a compliance module in your electronic health record (EHR). It could be a purpose-built HIPAA compliance tool. It could be a well-structured SharePoint site with clear folder conventions and named owners. The tool matters less than the discipline of only having one. When a renewal questionnaire arrives, and the administrator must decide "where is this documented," every additional guess is a defect that slows the response.

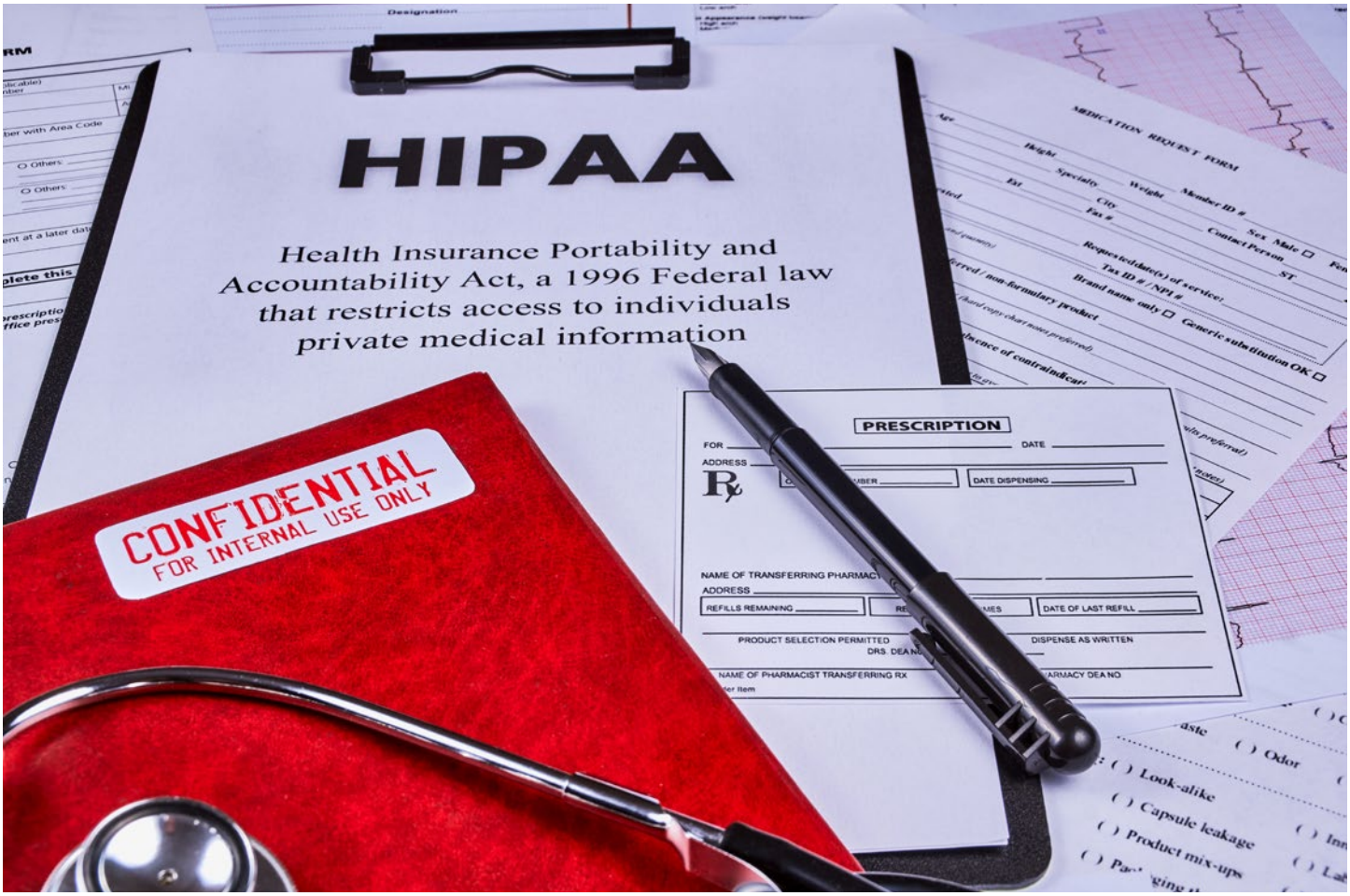
Carriers increasingly require documented evidence of controls before binding coverage.

3. Make training prove itself

Annual HIPAA training is a hard requirement. Nearly every small practice I audit has done the training. Not everyone can show me the completion logs with dates, employee names, and the specific training module.

Whatever system delivers the training should also log it, ideally to the same system of record from step two. If your training vendor does not export completion data cleanly, switch

Reprinted with permission. Copyright © 2026 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA).



vendors. That is cheaper than one citation. The completion log should include the employee's name, role, the module title and version, the date completed, and a signed acknowledgment that the employee understood the content. That signed acknowledgment is what stands up under audit.

4. Run a monthly access review in 15 minutes

Pull the list of users with access to PHI from your EHR and any downstream systems: billing, scheduling, imaging, patient portal, revenue cycle tools. Compare it to your current staff roster. Anyone on the access list who is no longer on staff gets deactivated that day, and the review gets signed off.

Fifteen minutes a month is less than what most practices spend on a single unscheduled access audit during an insurance renewal. The signed-off monthly review also creates a month-by-month paper trail that turns an ad hoc task into documented ongoing activity, which is what OCR expects.

5. Capture incidents as they happen, not when they are discovered

A lost laptop. A misdirected email with PHI. A phishing attempt that succeeded against one staff member. These are incidents whether they rise to the level of a reportable breach or not.

Small practices tend to have private conversations about incidents instead of documented ones. Document every incident, even minor, and decide deliberately whether each one requires notification under the Breach Notification Rule.[5] The documented decision is the defense if it ever becomes a question. An undocumented decision that turned out to be right is worth nothing in an investigation. A documented decision supported by a contemporaneous risk analysis is often the difference between a small finding and a six-figure settlement.

6. Build a one-page audit-readiness dashboard

This is the payoff. Every artifact from step one becomes a row. Each row shows where it lives, when it

Reprinted with permission. Copyright © 2026 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA).

was last updated, and who owns it. When the cyber insurance questionnaire lands, or OCR calls, or a client asks about your BAAs, you open one view, and everything is current.

That is what audit-ready looks like: a single view you can open instead of a scramble you have to run. The specific tools vary by practice. What does not vary: the shift from "we do the work" to "we can prove the work" is less about adding effort and more about redirecting effort that is already happening into a single, visible system.

The transformation

That practice administrator I mentioned at the beginning, the one who spent three weeks pulling records for her cyber insurance renewal, ran her next renewal in a single afternoon. She did not start doing more. She started doing the same things in one place. When her next OCR-adjacent question came up, she opened her dashboard, exported three artifacts, and sent them the same day.

The scramble is gone. Her premium came down at the following renewal because the "unable to verify" markers were all replaced with dated, signed proof. None of her actual work had changed. What changed was that she could finally see it. For practices that implement this approach, the difference is not measured in hours saved during an audit; it is measured in whether the audit becomes an ordinary event or a crisis.

Conclusion

HIPAA does not penalize practices for being imperfect. It penalizes practices that cannot produce evidence of reasonable diligence. For small practices operating without a dedicated compliance officer, the highest-leverage move is not adding more controls but making the ones they already run visible, dated, signed, and retrievable. The six-step system previously discussed is the operational version of that principle. Implemented once, maintained monthly, it converts compliance from an annual scramble into a running log that defends itself. CT

Endnotes

1. 45 C.F.R. § 164.316(b)(1), https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.316#p-164.316(b)(1).
2. 45 C.F.R. § 164.316(b)(2)(i), https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.316#p-164.316(b)(2)(i).
3. U.S. Department of Health and Human Services, "Resolution Agreements and Civil Money Penalties," content last reviewed September 17, 2026, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.
4. Office of the National Coordinator for Health Information Technology and Office for Civil Rights, "Security Risk Assessment Tool," last updated September 18, 2026, https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool.
5. 45 C.F.R. § 164.404, https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D/section-164.404.

Takeaways

- The U.S. Department of Health and Human Services Office for Civil Rights and cyber insurers penalize practices that cannot prove compliance, not practices that are imperfect but well-documented.
- Documentation required by the HIPAA Security Rule must be retained in written form for a minimum of six years from its last effective date.
- Small practices typically fail HIPAA audits and insurance renewals because of invisible documentation, not negligence or absent controls.
- The highest-leverage fix is picking one system of record and moving every compliance artifact into it before adding any new tools.
- A monthly 15-minute access review creates the ongoing documented activity that HIPAA enforcement expects and renewal questionnaires require.

Reprinted with permission. Copyright © 2026 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA).