New HIPAA Compliance Cost Benchmark Estimates $9,500 in Annual Staff Time for 10-Person Practices

Preliminary findings estimate $9,500 in annual staff-time burden; Patient Protect is removing one recurring cost for 50 practices.



Secure Care Research Institute estimates that a 10-person independent healthcare practice absorbs about $9,500 per year in recurring HIPAA compliance staff time.

CHICAGO, IL, UNITED STATES, September 30, 2026 / EINPresswire.com/ -- How much does HIPAA compliance cost in 2026? Preliminary findings from a forthcoming Secure Care Research Institute benchmark estimate about $9,500 per year in recurring staff-time cost for a 10-person independent healthcare practice — before dedicated compliance software, consultants, security technology, remediation, legal work or incident response.

The benchmark, “How Much Does HIPAA Compliance Cost in 2026? The Administrative Cost of Compliance for Independent Healthcare Practices,” estimates $9,471 in annual recurring administrative work under its base assumptions. When the model substitutes narrower federal documentation estimates for its two largest workload assumptions, the result is still about $6,800.

> “HIPAA doesn’t send an invoice. It sends work to be done. For a small practice, that work gets absorbed by people who already have another job like caring for patients.”
>
> *Alexander Perrin, Co-Founder & CEO, Patient Protect*

The full paper is in final production. The findings, methodology, limitations and publisher disclosure are available now.

What HIPAA compliance costs before anything goes wrong

HIPAA does not charge a practice one annual fee. The cost shows up in the work: risk analysis, risk management, policies, workforce training, access administration, vendor oversight, incident readiness, system activity review and documentation.

For the 10-person base case, the model assigns 121.5 hours of recurring manager time plus 20 hours of staff time each year, valued using Bureau of Labor Statistics wage and compensation data.



Patient Protect is offering one year of HIPAA Foundations training at no cost to up to 50 independent healthcare practices, including 19 modules, 95 assessment questions, and training for up to 25 personnel.

The burden falls especially hard on the smallest practices. The model estimates $7,937 in recurring annual administrative cost for a three-person practice, or $2,646 per workforce member. At 40 people, the modeled total rises to $16,894, but the burden falls to $422 per person — more than a sixfold difference.

“HIPAA doesn’t send an invoice. It sends work to be done,” said Alexander Perrin, co-founder and CEO of Patient Protect. “For a small practice, that work gets absorbed by people who already have another job, like tending to patients. The purpose of the research was to make that cost visible before considering software, penalties or ROI.”

The research does not present $9,471 as a national average or as the total cost of HIPAA compliance. It is an activity-based estimate of recurring administrative work.

What happened when smaller providers faced HIPAA enforcement

The Institute also asked: when smaller healthcare organizations ended up in serious Security Rule enforcement, what did regulators actually cite?

Researchers reviewed 133 monetary HIPAA resolutions listed by the U.S. Department of Health and Human Services Office for Civil Rights through the study’s August 27, 2026 data cutoff. After narrowing the record to independent practices and other qualifying smaller providers, the study identified 16 monetary Security Rule actions.

In all 16, OCR cited the HIPAA risk-analysis provision.

That does not mean every independent practice has a deficient risk analysis or a known chance of being fined. OCR also has an enforcement initiative focused on risk-analysis compliance,

which can affect case selection. The pattern nevertheless appeared both before and after OCR publicly described that initiative in April 2024: seven of seven qualifying actions before and nine of nine after.

Among the 15 settlements in that group, the median payment was $103,000, with settlements ranging from $10,000 to $1.5 million. Every settlement also required an HHS-monitored corrective action plan; 14 lasted two years and one lasted three.

Those plans can require organizations to repeat risk analysis, revise policies, retrain staff, document remediation and report progress back to HHS.

The research does not present $103,000 as an expected HIPAA fine. The takeaway is simpler: compliance takes work before anything goes wrong, and when regulators step in, the work can become more expensive, more urgent and externally supervised.

Patient Protect is removing one piece of that burden for 50 practices

Publishing research about the cost of compliance is useful. Reducing some of that cost is better.

Workforce training is one of the recurring responsibilities every HIPAA program has to manage. For a small practice, training is not just the cost of a course. Someone has to assign it, track who finished it, retain the records and be able to prove completion later.

That is why Patient Protect is extending its HIPAA Training Access Initiative through November 30, 2026 and making its complete HIPAA Foundations training program free for one year to up to 50 U.S. independent healthcare practices.

“Publishing research showing how much work small practices absorb should be followed by action,” Perrin said. “Training is one recurring piece of the burden that can be taken off the budget immediately. For 50 practices, that is exactly what Patient Protect is doing.”

Selected practices receive the full Foundations program for up to 25 personnel: 19 training modules, approximately 1 hour and 41 minutes of expert-led instruction, 95 scored knowledge-assessment questions, individual learner accounts, administrator progress and score tracking, downloadable office-level reports and QR-verifiable Certificates of Completion.

Most HIPAA training stops at one question: did the employee finish?

Patient Protect is designed to answer more useful questions: what did they learn, did they pass, who is finished, who is overdue and can the practice prove it later?

“A completion certificate shows that someone finished. It does not show what the employee

understood or whether the practice can produce the record later," said Angie Perrin, RDH, CHPC, co-founder and Chief Security Officer of Patient Protect. "Training Foundations was built to leave both knowledge and evidence behind."

There is no automatic conversion to a paid Patient Protect subscription and no requirement to provide a public review, testimonial or endorsement. Applications and rolling selection remain open through November 30, 2026.

About Patient Protect

Patient Protect is a security-first HIPAA compliance platform built for independent healthcare practices. It brings risk analysis, risk management, policies, workforce training, vendor and business associate management, compliance evidence, secure workflows and ongoing security operations into one connected operating system for working compliance.

About Secure Care Research Institute

Secure Care Research Institute is the research unit of Patient Protect LLC. Its work examines healthcare data exposure, HIPAA enforcement, cybersecurity economics and the operating burden of protecting electronic protected health information.

Alexander J. Perrin
Patient Protect
info@patient-protect.com
Visit us on social media:
LinkedIn
Instagram
YouTube
X

This press release can be viewed online at: https://www.einpresswire.com/article/946198192

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.