



Penetration Testing Services for HIPAA Compliance

Steps to Schedule Your HIPAA Penetration Test:

- ▶ Schedule a 30-minute Discovery Session
- ▶ We determine IF and HOW we can help
- ▶ We provide a Tailored Proposal
- ▶ Together, we review the Proposal

Medical information is highly valuable – perhaps more profitable to hackers than credit card data. It often includes social security numbers, birth dates, insurance numbers, diagnosis codes, and billing information. Hackers can use this data to commit identity fraud and to secure false prescriptions. It is vital that medical institutions perform regular pen testing to assure themselves, their clients, and their regulatory agencies that data is safe from prying eyes.

HIPAA (Health Insurance Portability and Accountability Act of 1996) is the US federal law that governs the privacy, safety, and electronic exchange of medical information. As part of remaining compliant with HIPAA, medical institutions must perform regular technological tests of their data security. What better way to test a system than to think like the person hacking it? That's what our penetration test for HIPAA compliance tests.



Specifically, HIPAA Evaluation Standard § 164.308(a)(8) applies to penetration testing:

- ▶ A covered entity or business associate is required to perform a periodic technical and nontechnical evaluation.
- ▶ A technical evaluation is typically defined as performing a vulnerability assessment or a penetration test.

Essentially, the technical evaluation provides validation that the controls defined in the documentation are actually implemented effectively and working as described. The nontechnical evaluation assesses the plan on paper, whereas the technical evaluation assesses the plan's implementation. An independent third party should perform the technical evaluation.

Additionally, NIST issued guidance (NIST 800-66) for HIPAA that states:

“Conduct penetration testing (where trusted insiders attempt to compromise system security for the sole purpose of testing the effectiveness of security controls), if reasonable and appropriate.”

Although HIPAA only recommends a penetration test be performed annually, we recommend a quarterly program that includes validation testing.

Contact us for a no-cost consultation on our
HIPAA penetration testing services.

Blue Goat Cyber

PO Box 20310

PMB 45092

Cheyenne, Wyoming 82003-7007

☎ (307) 317-8884

✉ info@bluegoatcyber.com