Is Your Health Data Protected the Way the Law Requires?

Gap assessment across 24 HIPAA Security Rule controls - administrative, physical, technical and organizational safeguards - for US covered entities and business associates handling ePHI.

IN SHORT

Covers the Administrative (§164.308), Physical (§164.310), Technical (§164.312), Organizational (§164.314) safeguards and the Policies/Documentation requirement (§164.316) of the HIPAA Security Rule.

24	4	US
HIPAA Security Rule controls covered	Safeguard categories: administrative, physical, technical, organizational	Covered entities and business associates with ePHI access

THE SITUATION TODAY

WHO YOU ARE

You're the security or compliance lead of a US covered entity or business associate handling electronic protected health information (ePHI) that needs to demonstrate Security Rule compliance.

WHAT HAPPENED

An audit, a healthcare client, or a business associate agreement asks for evidence of the Security Rule's administrative, physical, and technical safeguards.

WHY IT HURTS

HIPAA penalties for violations can reach over $1.5M per year per violation category, on top of the reputational damage in a high-sensitivity sector like healthcare.

WHERE YOU WANT TO GET TO

DESIRED OUTCOME	You want to know, control by control, what's satisfied, what's partial, and what's missing - with real technical evidence attached to every answer, not an optimistic claim nobody has verified.
THE SOLUTION	Pentesterra's HIPAA Security Rule Gap Assessment: a structured assessment across every control, with technical controls auto-filled from vulnerability scanning, penetration testing, OSINT and External Exposure monitoring wherever evidence exists.
WHY IT'S DIFFERENT	You're not buying another self-assessment questionnaire, and this isn't a legal opinion. You're working with [YOUR COMPANY NAME] - a certified provider with a long track record in information security. You've likely worked with us already, directly or through someone you know - a colleague, a supplier, a competitor. And the gap assessment doesn't stop at a paper checklist: technical controls are auto-filled from evidence already on file, with cross-standard mapping to the other 12 frameworks the platform supports, so a second audit never starts from zero.
CONCRETE PROOF	The result is a complete, ready-to-deliver PDF report covering every control, with a direct reference to the legal/regulatory basis. If gaps come up, we propose the additional services to close them: vulnerability assessment, network or application penetration testing, phishing training and simulation.

WHAT'S ACTUALLY INCLUDED

Not a generic checklist - the real controls of HIPAA Security Rule, grouped the way you'll see them in the platform.

Administrative Safeguards (§164.308)

The largest group: governance, training, access management.

- Risk analysis and risk management
- Security awareness and training
- Incident response and contingency planning

Physical Safeguards (§164.310)

Control of physical access to facilities and devices.

- Facility access controls
- Workstation and device security
- Secure media disposal and re-use

Technical Safeguards (§164.312)

The technical controls directly verifiable on systems handling ePHI.

- Access control and unique user authentication
- Encryption of data in transit and at rest
- Audit logs and integrity controls

Organizational and Documentation (§164.314, §164.316)

The contractual and documentation obligations.

- Compliant business associate agreements
- Documented policies and procedures
- Compliance records maintained over time

WHAT YOU GET

- ✓ An exportable XLSX control matrix, with the status of every individual control
- ✓ An editable DOCX gap report, ready for your auditor or your board
- ✓ Technical controls auto-filled from evidence the platform already collected
- ✓ Guided applicability check by sector, country, and company size
- ✓ Cross-standard mapping to the other 12 frameworks the platform supports - answer once, reuse across standards
- ✓ A one-click auditor package: questionnaire, technical evidence and gap report together
- ✓ Prioritized remediation recommendations for the gaps found

HOW IT WORKS

1

We define the scope

Assessment boundary, systems and processes involved - we set the scope together.

2

We collect the evidence

Technical controls are auto-filled from evidence the platform already collected.

3

We complete the questionnaire

Non-technical controls are verified with your team.

4

We deliver the report

A complete PDF with the gaps found and the actions to take.

Find out how ready you are for HIPAA Security Rule

A complete report, ready to present to clients, auditors, or your board.

Request your HIPAA Security Rule Gap Assessment →

info@pentesterra.com · pentesterra.com/solutions/compliance