CYBERNOUS™
INFOSEC CONSULTING

HIPAA Simplified for All Security Professionals

Join us as in break down HiPAA with expert guidance to to ensure your compliance journey is smooth and impactal.

Ready to dive in? Swipe to get started!

CYBERNOUS™
INFOSEC CONSULTING

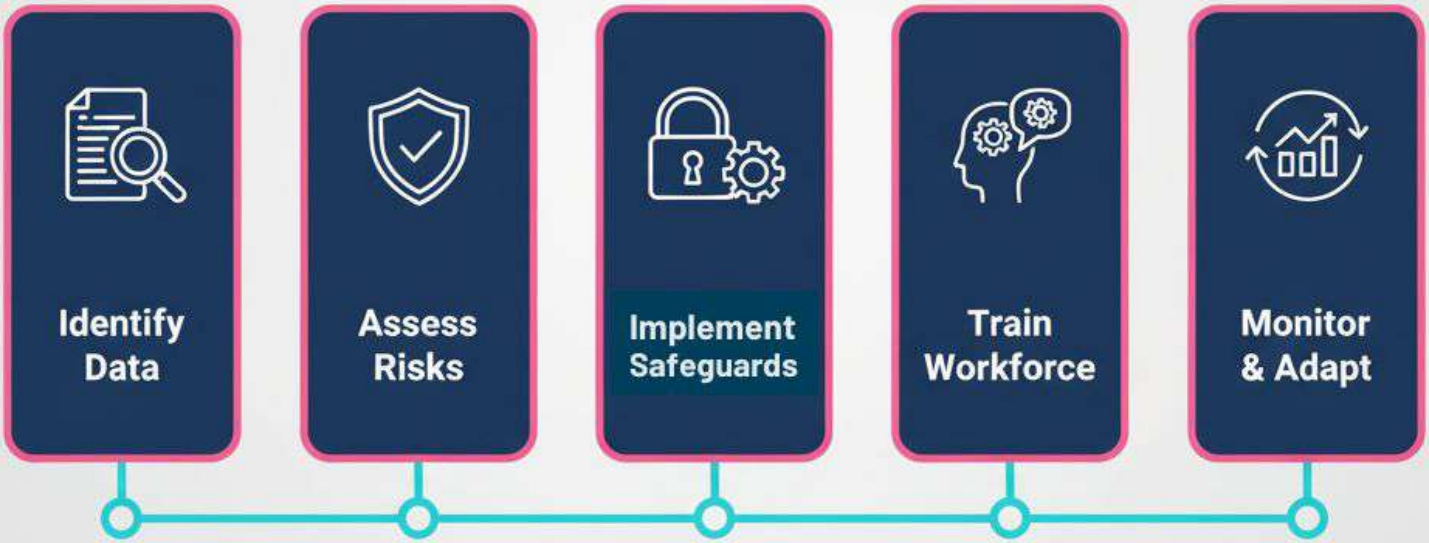
What is HIPAA?

HIPAA protects patient health information. It ensures data privacy and sets standards for safugraging PHI across healthcare organizations.

CYBERNOUS™
INFOSEC CONSULTING

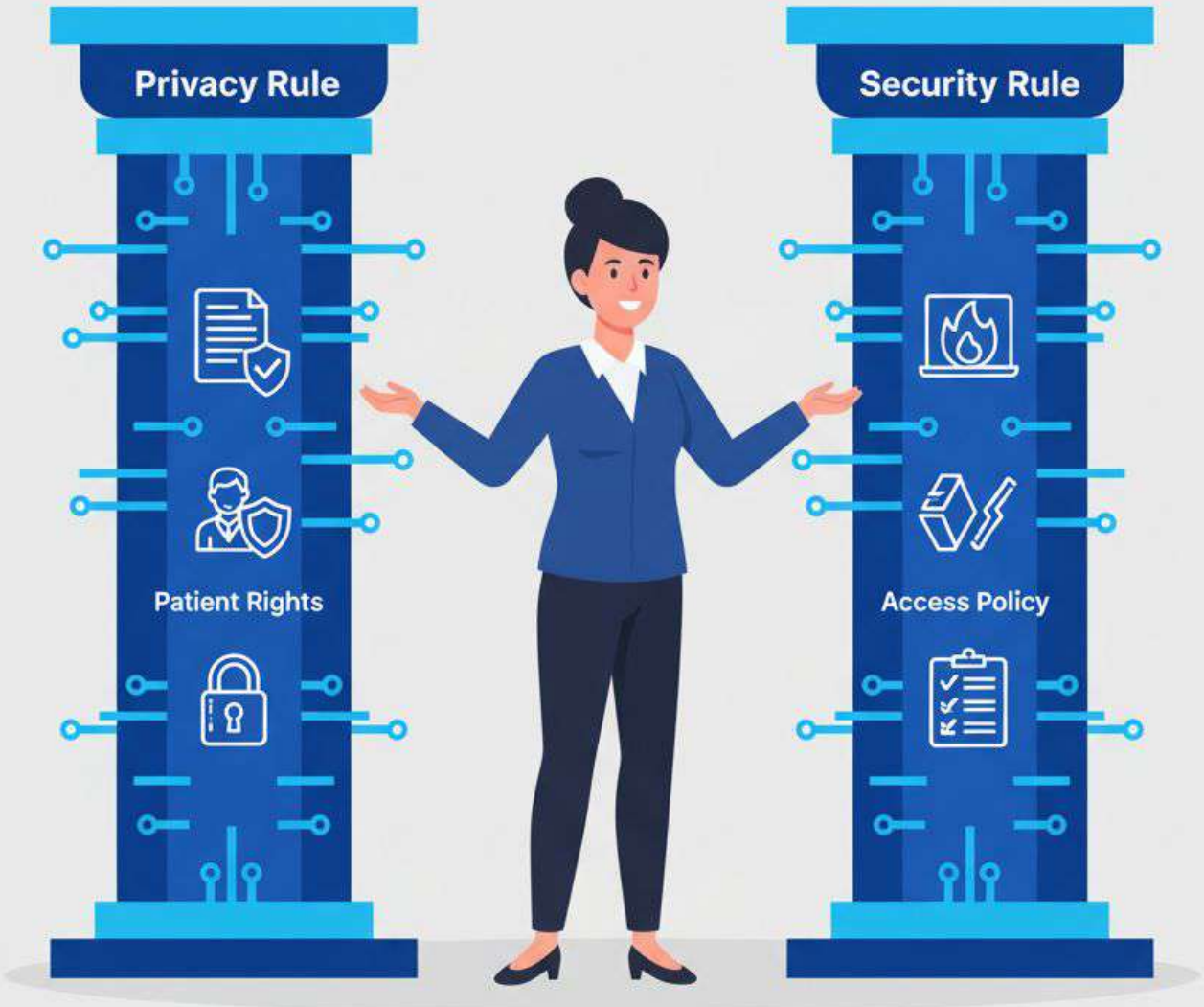
How to Get Compliant with HIPAA

To become compliant with HIPAA, you must map your data, implement safeguards, and train your workforce to continuously assess and protect Protected Health Information (PHI).



CYBERNOUS™
INFOSEC CONSULTING

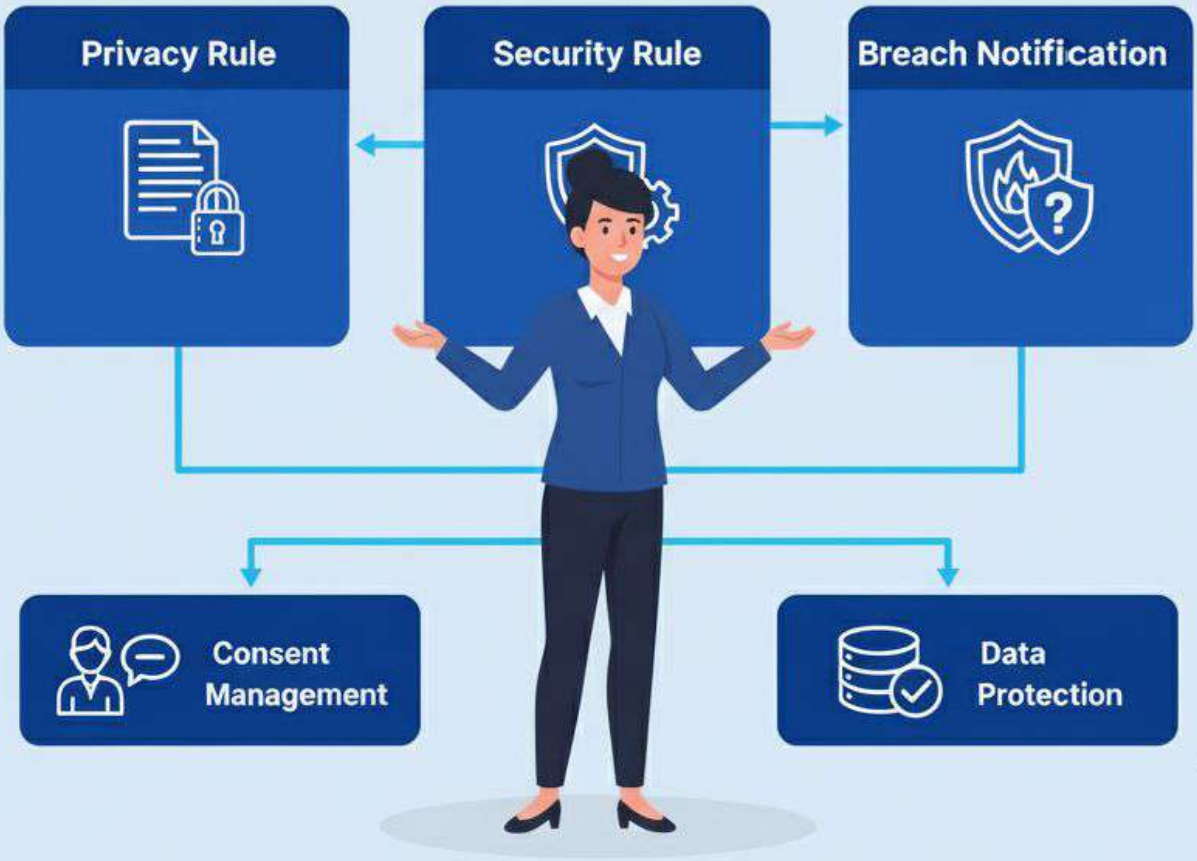
The Two Pillars of HIPA



CYBERNOUS™
INFOSEC CONSULTING

Key Provisions of HIPAA (Major Requirements)

HIPAA covers Privacy, Security, and Breach Notification rules to protect Protected Health Information (PHI). It ensures the security of electronic PHI (ePHI) and regulates how all PHI is used and disclosed.



CYBERNOUS
INFOSEC CONSULTING

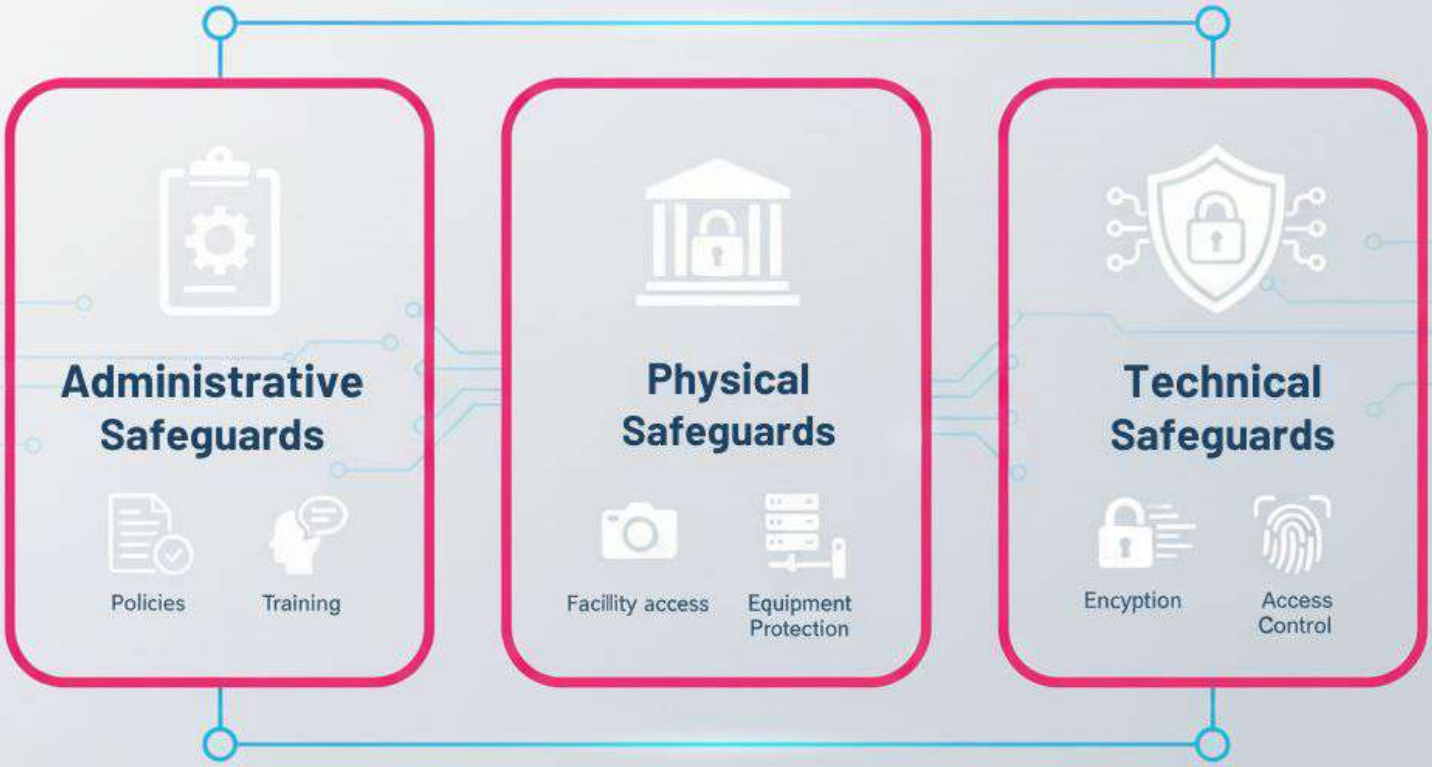
Strategy for HIPAA Adoption

Adopt HIPAA by establisling leadership commitment, creating a governance framework, and implementing risk mitigation strategies to ensure continuous compliance.

CYBERNOUS™
INFOSEC CONSULTING

Compliance Requirements & Mandatory Requirements

Compliance requires administrative, physical, and technical safugrards to protect PHI. These inclutecrytion, access control, and workforce training.




CYBERNOUS
INFOSEC CONSULTING
HIPAA PRIVACY RULE
YOUR DATA RIGHTS
Consent for:
Treatment
Payment
Sharing

CYBERNOUS™
INFOSEC CONSULTING

The "Oh No!" Plan: Breach Notification 🔥

A data breach triggers the clock! We must notify affected parties and HHS. Thanks to the **HITECH Act** and the **Omnibus Rule**, a breach is presumed reportable unless we can demonstrate a low probability of compromise. A solid **Incident Response Plan** is critical.

CYBERNOUS™
INFOSEC CONSULTING

Trusting Our Partners:
Business Associate Agreements (BAs) 👍

We don't work alone. We share PHI with third parties, called Business Associates. A **Business Associate Agreement (BAA)** is a legally required contract ensuring they protect the data. It extends our security perimeter and makes them directly liable for **HIPAA violations.**

CYBERNOUS™
INFOSEC CONSULTING

The Stakes: Civil and Criminal Penalties

CIVIL Penalties
(The value every GRC pro must understand.)

CRIMINAL
(Handled by the Department of Justice)

Violations aren't taken **lightly**. The Enforcement Rule outlines two tiers of penalties every **GRC professional** must understand.

Civil Penalties:
Range from $100 to $50,000 per violation, with an annual maximum of $1.5 million for repeat violations, depending on the level of negligence.

Criminal Penalties
For "knowing" violations, handled by the Department of Justice:

- Up to **$50,000 & 1 year in prison** for knowingly obtaining/disclosing PHI.
- Up to **$100,000 & 5 years** for offenses committed under false pretenses.
- Up to **$250,000 & 10 years** for offenses committed with the intent to sell, transfer, or use PHI for malicious harm or gain.

Follow Us to Learn More...

Want more insights into HiPPA compliance strategies and breach prevention?

Follow us for updates and expert guidance on staying compliant!