HIPAA Compliance Architecture

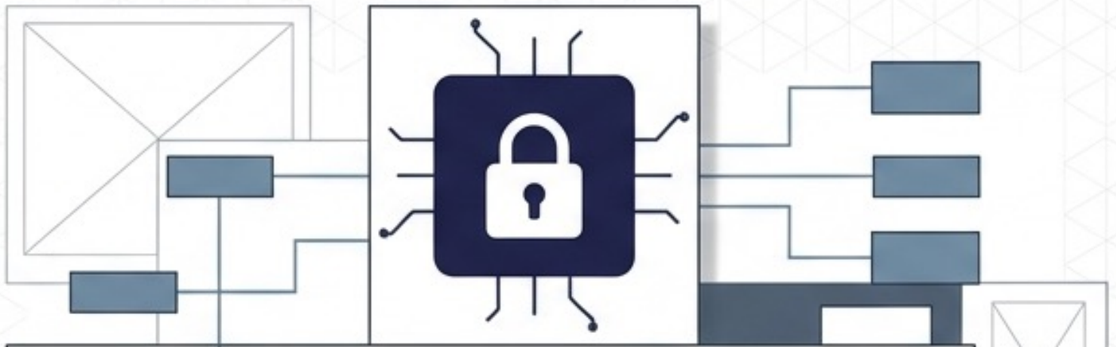
A Strategic Blueprint for Data Governance, Privacy, and Cybersecurity

The Dual Mandate of Protected Health Information

HIPAA establishes federal standards protecting sensitive health information from disclosure without patient consent while allowing necessary access to promote high-quality healthcare.

The Privacy Rule

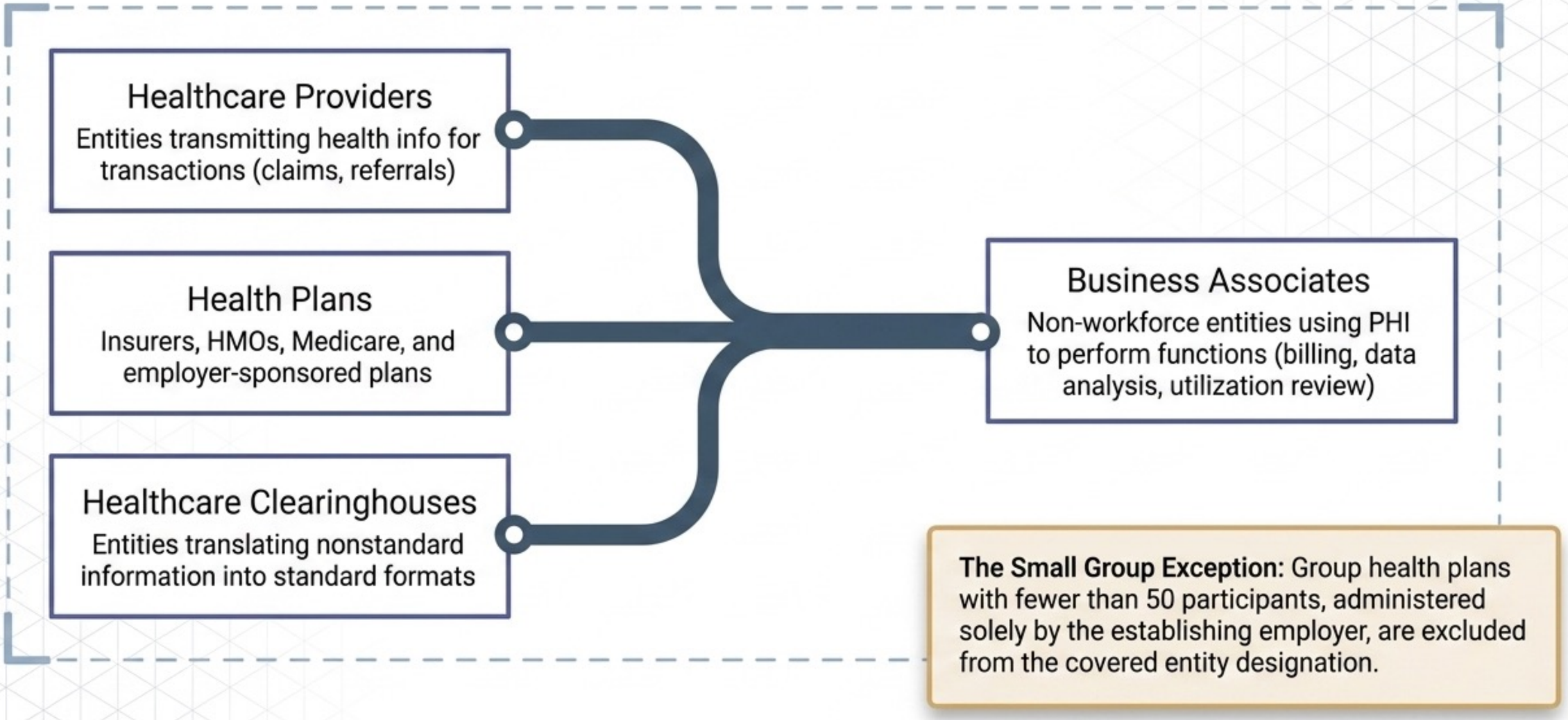
Addresses the broad use and disclosure of individuals' protected health information (PHI) and establishes the right to understand and control how health data is used.



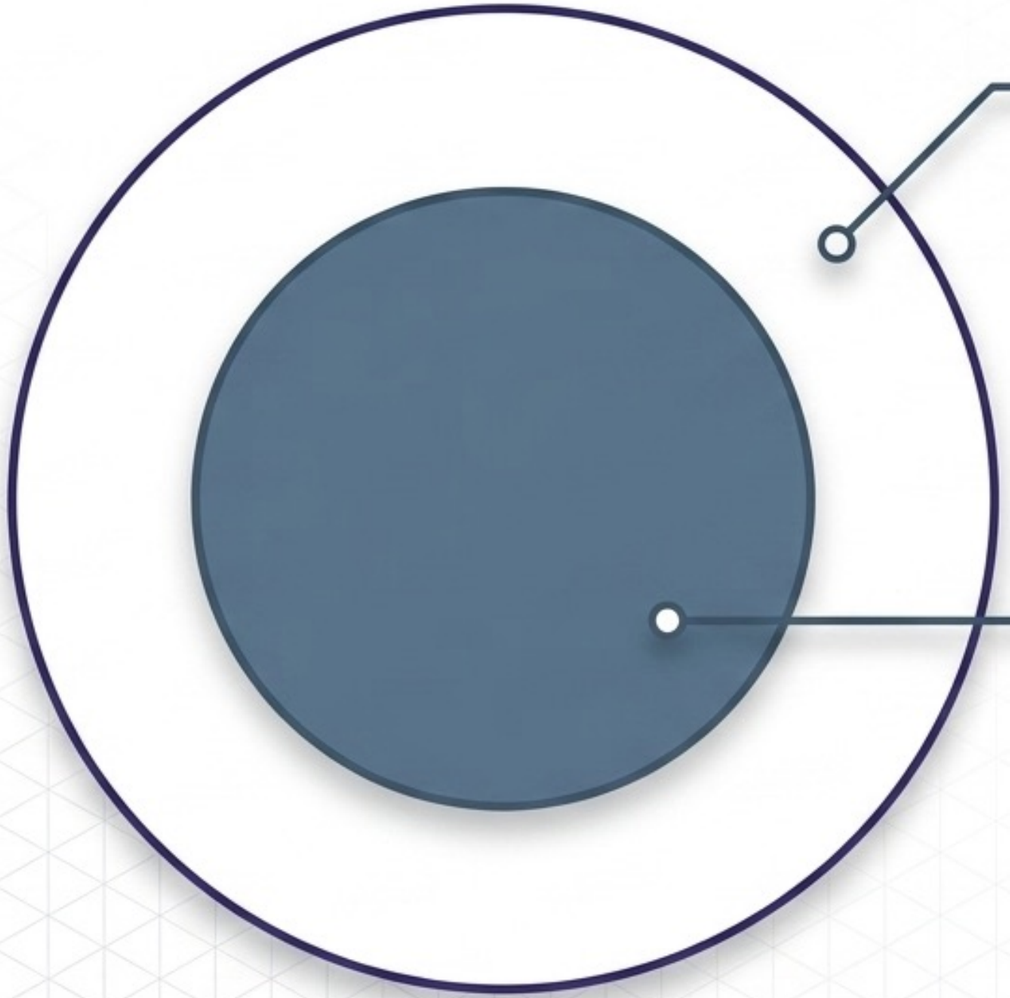
The Security Rule

Strictly protects a specific subset of data covered by the Privacy Rule, enforcing cybersecurity safeguards for information transmitted or maintained in electronic form.

The Scope of Governance: Covered Entities



The Core Asset: Isolating e-PHI



Protected Health Information (PHI)

Encompasses all individually identifiable health information regardless of medium—-including data transmitted orally or in writing. Governed by the Privacy Rule.

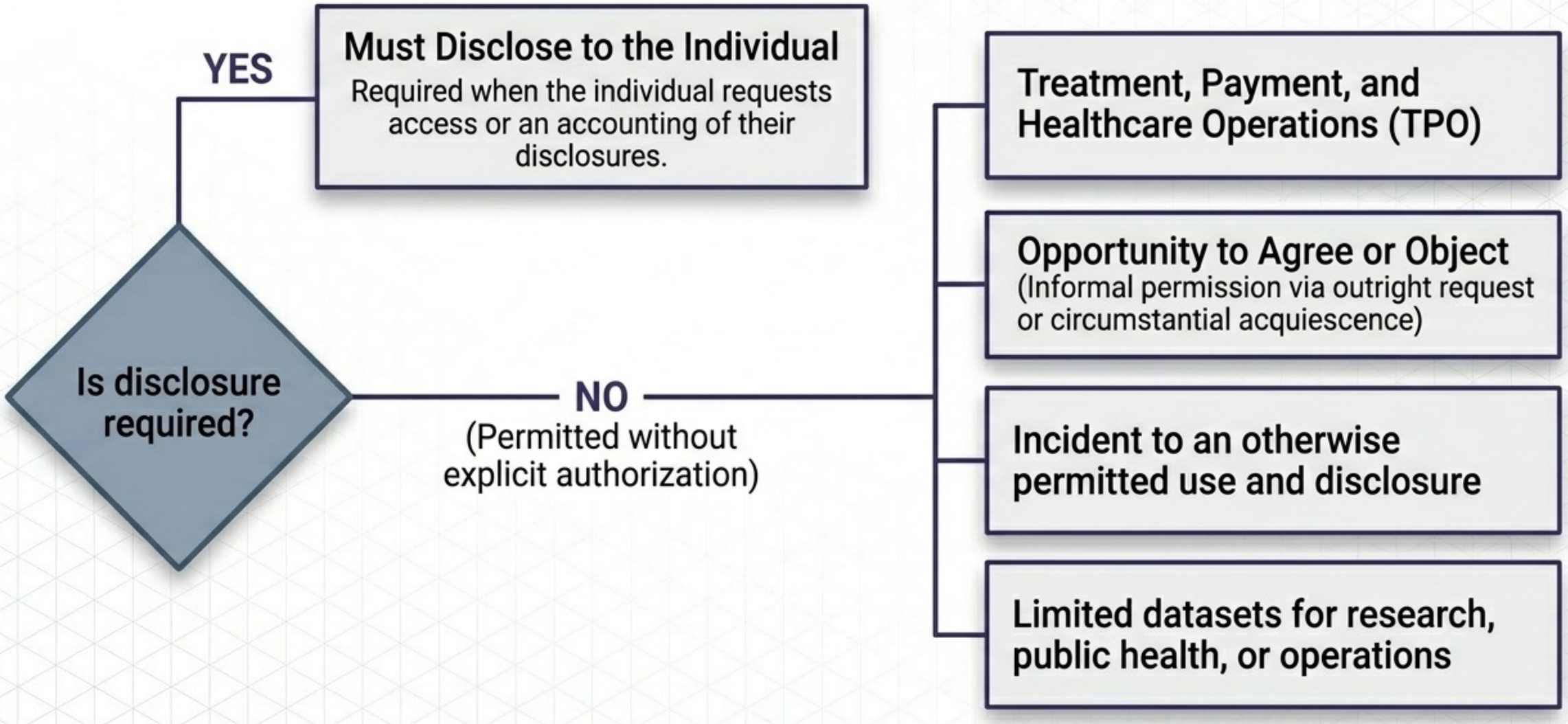
Electronic Protected Health Information (e-PHI)

A strictly defined subset of PHI that a covered entity creates, receives, maintains, or transmits in electronic form. Governed by the Security Rule.

Diagnostic Comparison: Privacy vs. Security Standards

	The Privacy Rule	The Security Rule
Regulated Asset	All Protected Health Information (PHI)	Electronic Protected Health Information (e-PHI) only
Primary Objective	Control, patient consent, and regulating disclosure	Cybersecurity safeguards, threat detection, and data preservation
Regulated Medium	Oral, Written, and Electronic	Electronic only

The Privacy Rule Framework: Permitted Disclosures



12 National Priority Disclosures

The Privacy Rule permits use and disclosure of PHI without authorization for the following public interest and benefit activities:

- Required by law
- Public health activities
- Victims of abuse, neglect, or domestic violence
- Health oversight activities
- Judicial and administrative proceedings
- Law enforcement
- Deceased persons (identification functions)
- Cadaveric organ, eye, or tissue donation
- Research (under specific conditions)
- Prevention of serious threat to health or safety
- Essential government functions
- Workers' compensation

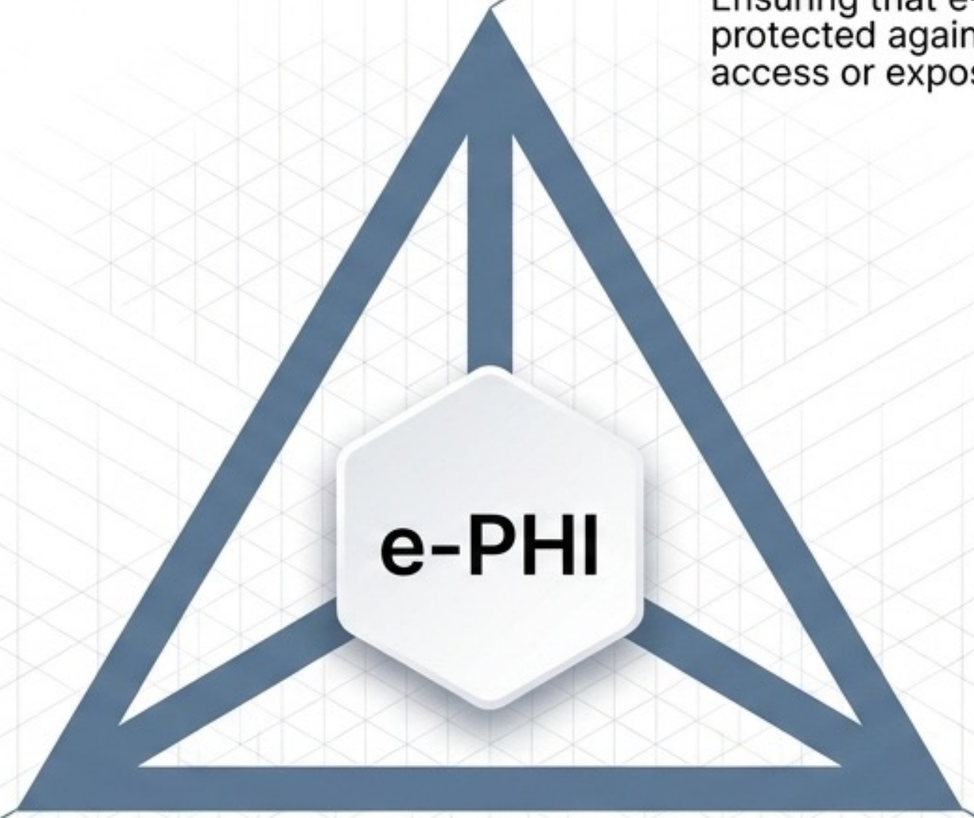
The Cybersecurity Mandate

While the HIPAA Privacy Rule safeguards PHI, the Security Rule protects a subset of information...

To comply, all covered entities must actively ensure the defense of e-PHI against anticipated threats and impermissible uses.

The e-PHI Security Engine

Statutory mandate to ensure three core pillars of data security.



Confidentiality
Ensuring that e-PHI is protected against unauthorized access or exposure.

Availability
Ensuring that authorized healthcare providers and systems can reliably access e-PHI when needed.

Integrity
Safeguarding the data to ensure it is not improperly altered or destroyed.

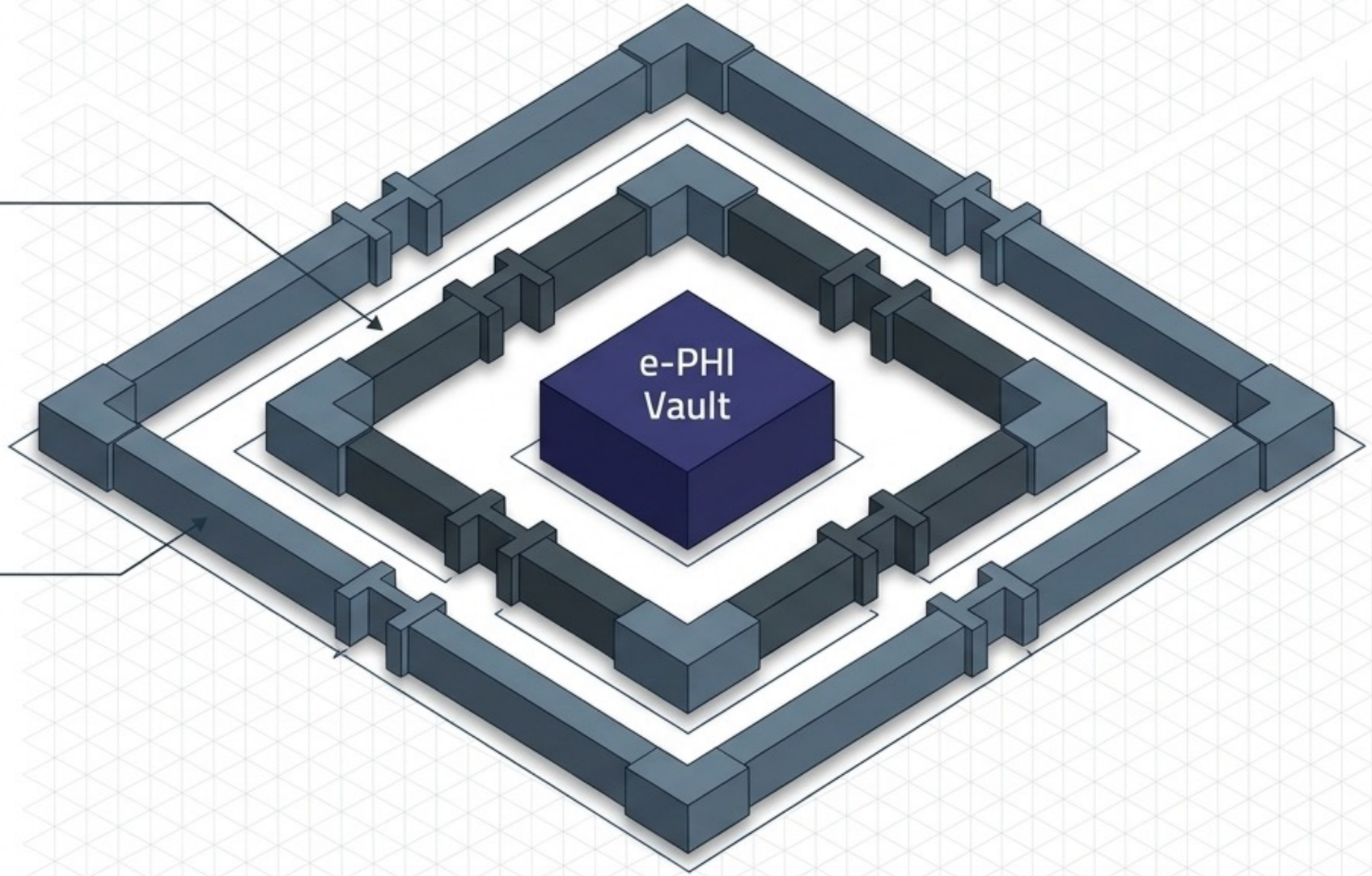
Threat Defense & Active Safeguards

Safeguard against anticipated threats.

Systems must be in place to detect and neutralize anticipated threats to the security and integrity of the information.

Protect against impermissible uses.

Robust access controls must actively protect against anticipated impermissible uses or disclosures that are not allowed by the rule.



Governance in Action: The Human Element

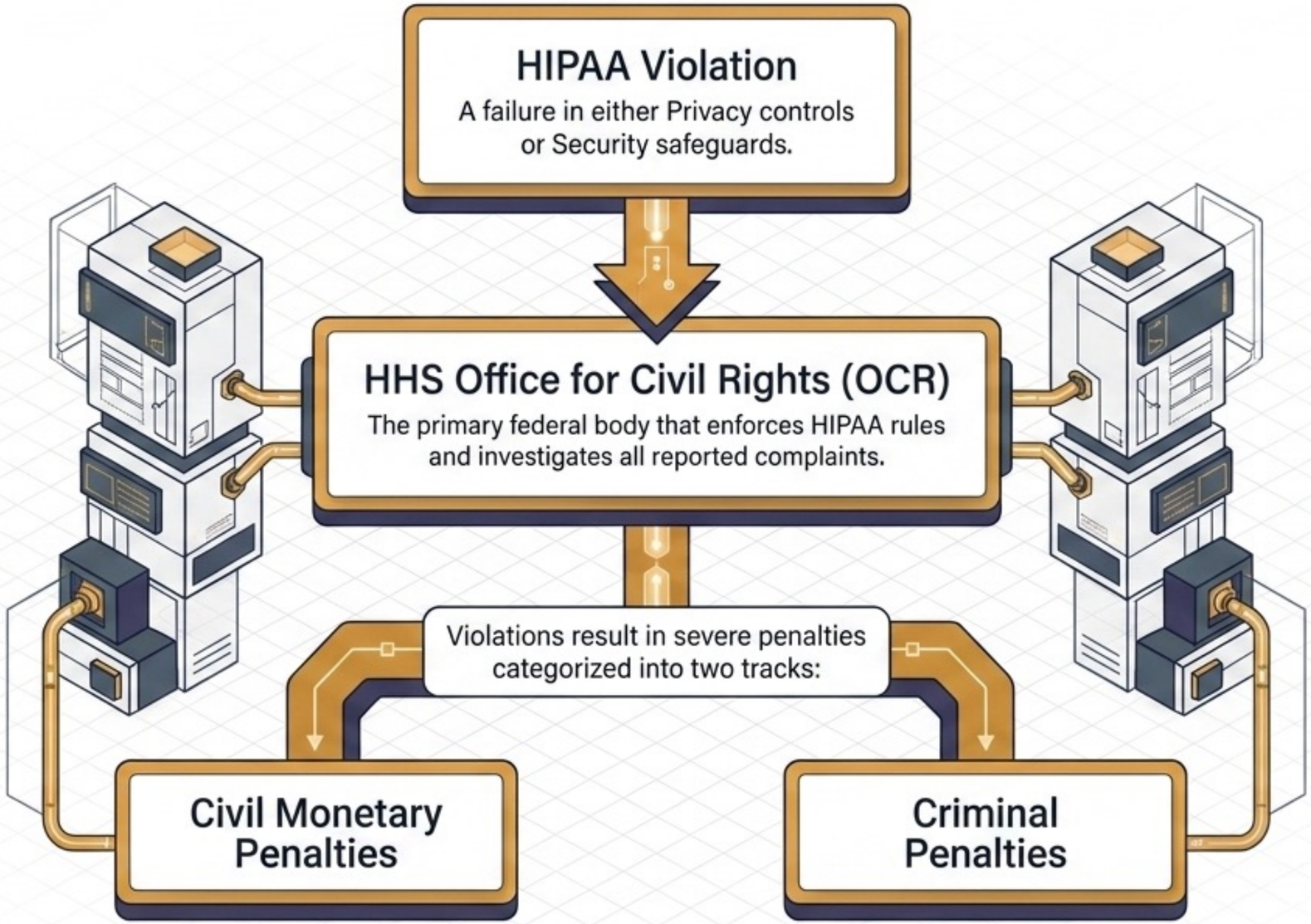
Workforce Certification

Covered entities are strictly required by the Security Rule to actively certify compliance across their entire workforce. Technology alone is insufficient without trained operators.

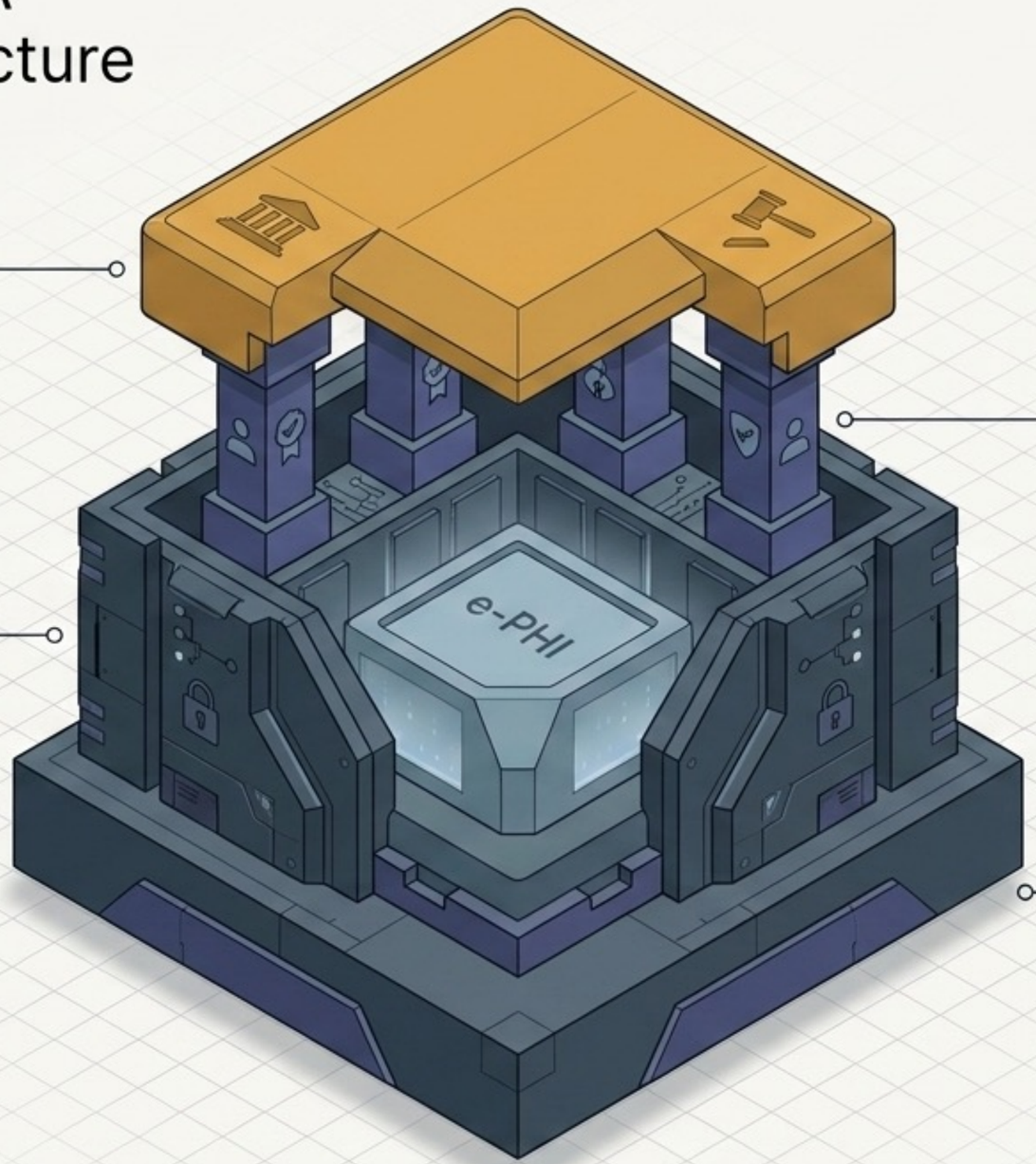
Professional Ethics

When evaluating requests for permissive uses and disclosures, covered entities must rely heavily on professional ethics and best judgment to ensure compliance aligns with patient care.

Accountability & Enforcement



The Complete HIPAA Governance Architecture



Federal Accountability
OCR enforcement enforcing civil and criminal compliance.

Security Safeguards
Active defense mechanisms ensuring Confidentiality, Integrity, and Availability of electronic data.

Human Governance
Workforce certification and ethical application of permissive uses.

Privacy Baseline
Broad protections for all forms of PHI and patient consent.