HIPAA IT SECURITY

Ongoing Execution & Oversight

HIPAA IT SECURITY

Ongoing Execution
& **Oversight**

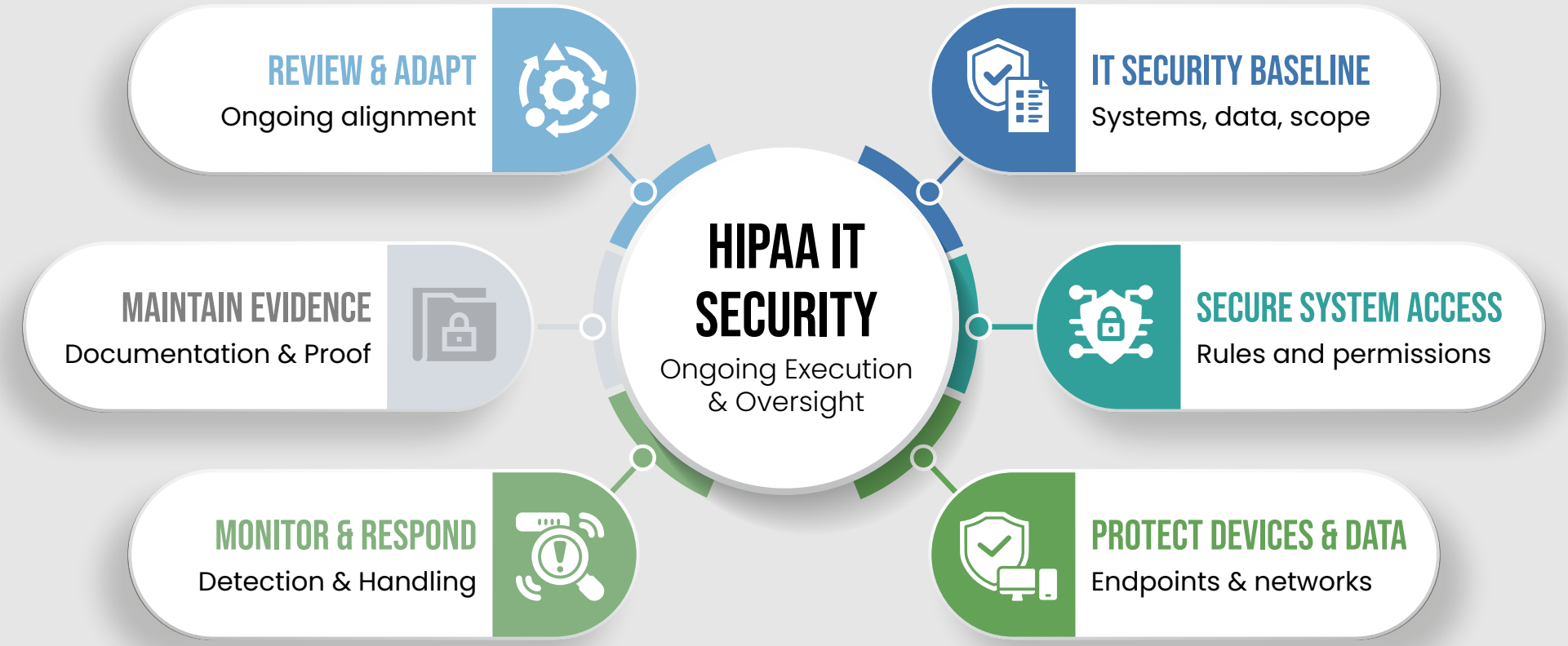
THE HIPAA IT SECURITY EXECUTION PROCESS

HIPAA IT security is not a project you complete once.
It is an ongoing operational responsibility tied to **systems**, **access**, and **data**.

The process below is how we remove **ambiguity**, **reduce risk**, and take IT security oversight off the practice's plate, without disrupting clinical or administrative workflows.

HIPAA IT SECURITY

Ongoing Execution
& **Oversight**



STEP 1: THE HIPAA IT SECURITY EXECUTION PROCESS

We establish clear ownership and a documented IT security baseline for all systems that handle electronic protected health information **(ePHI)**.

We identify where ePHI exists, how it moves between systems, and which IT assets fall under **HIPAA** security requirements. This creates a clear, documented baseline that defines system scope, responsibility boundaries, and risk exposure related to IT.

This step ensures there is no ambiguity about what is covered, what is monitored, and who is accountable for **IT security execution**.

STEP 2: SYSTEM ACCESS & ENVIRONMENT HARDENING

Access to sensitive systems is restricted, monitored, and aligned with HIPAA technical safeguard requirements.

We implement and maintain access controls across systems that handle **ePHI**, ensuring users only have the access necessary for their role. System configurations are reviewed and hardened to reduce unnecessary exposure and limit the impact of compromised credentials or misuse.

This step focuses on preventing unauthorized access before it becomes an **incident**.

STEP 3: ENDPOINT, NETWORK & DATA PROTECTION

We secure endpoints, networks, and data paths to reduce the risk of unauthorized access or data exposure.

Workstations, servers, and network infrastructure are protected using layered security controls appropriate for **healthcare** environments. We focus on protecting data while it is being accessed, transmitted, or stored within IT **systems**.

Security is maintained continuously rather than relying on one-time configurations.

STEP 4: MONITORING, DETECTION & INCIDENT READINESS

Security events are continuously monitored, and incidents are handled using a defined, repeatable process.

We actively monitor **IT systems** for indicators of compromise, misconfiguration, or suspicious behavior. When events occur, they are evaluated, documented, and handled according to an established response process.

This ensures incidents are addressed consistently and with **proper documentation**, rather than reactively or informally.

HIPAA IT SECURITY

Ongoing Execution
& **Oversight**

STEP 5: IT DOCUMENTATION & EVIDENCE MAINTENANCE

We maintain the IT documentation and evidence typically requested during HIPAA inquiries or audits.

HIPAA enforcement focuses heavily on documentation and proof of ongoing security management. We maintain IT-specific records tied to **system security**, **risk findings**, **changes**, and monitoring activities.

This **documentation** demonstrates that **IT security** is actively managed over time, not assumed or delegated without oversight.

STEP 6: ONGOING OVERSIGHT & CHANGE MANAGEMENT

HIPAA IT security is maintained continuously as systems, staff, and threats change.

Healthcare IT environments change constantly. **New staff**, **new systems**, workflow changes, and evolving threats all affect risk.

We continuously review and adapt **IT security** controls to ensure they remain aligned with the practice's actual environment, rather than a **snapshot** in time.

HIPAA IT SECURITY

Ongoing Execution
& **Oversight**

WHAT THIS PROCESS IS (AND IS NOT)

This process is:

- Ongoing and operational
- Focused on IT security execution
- Designed to reduce oversight burden for practice leadership
- Built to support regulatory inquiries related to IT systems

This process is not:

- A one-time compliance project
- A checklist for staff to manage
- A replacement for legal or administrative compliance functions
- A set of generic “HIPAA-compliant” tools

HIPAA IT SECURITY

Ongoing Execution
& **Oversight**

HIPAA places responsibility on the practice, even when IT is outsourced.

This process exists to ensure the **IT security portion of that responsibility is owned, executed, and maintained consistently**, without requiring ongoing involvement from the doctor or staff.

If you want to understand how this **process** would apply to your specific **environment**, we are happy to walk through it together.

HIPAA IT SECURITY

Ongoing Execution
& **Oversight**

HIPAA places responsibility on the practice, even when IT is outsourced.

This process exists to ensure the **IT security portion of that responsibility is owned, executed, and maintained consistently**, without requiring ongoing involvement from the doctor or staff.

If you want to understand how this **process** would apply to your specific **environment**, we are happy to walk through it together.

HIPAA IT SECURITY

Ongoing Execution
& **Oversight**

If you want help understanding how HIPAA IT security execution applies to your specific practice, Asteroid IT offers a HIPAA Security Execution Readiness Call.

The session focuses on clarifying ownership, execution gaps, and documentation expectations based on how your practice actually operates.

Schedule your call: https://Asteroidit.com/hipaa-call

https://asteroidit.com
info@asteroidit.com
480-937-7021