THE PHOENIX PHYSICAL HIPAA SAFEGUARD AUDIT

Is your facility securing Patient Health Information (PHI) in the physical world?

Facility Name: _____ Date: _____ Auditor: _____

This self-assessment reviews compliance with the **Physical Safeguards** of the HIPAA Security Rule. While IT protects the firewall, this audit ensures the doors, screens, and servers are protected from physical theft and unauthorized viewing.

SECTION 1: FACILITY ACCESS CONTROLS (§ 164.310(a)(1))

Do you strictly limit physical access to electronic information systems?

- **[ ] The "Server Room" Standard**
  - Are servers containing ePHI housed in a locked room separate from general storage/janitorial supplies?
  - *Fail Point:* If the server rack is in an open office area or unlocked closet.
- **[ ] Validation Procedures**
  - Do you have a documented procedure to validate a person's authority *before* granting them physical access to restricted areas (e.g., ID Badge scanning + Guard Verification)?
- **[ ] Maintenance Records**
  - Are all repairs and modifications to physical security components (doors, locks, cameras) documented?
  - *Phoenix Tip:* Our guards maintain a real-time digital log of every maintenance vendor who enters your sensitive zones.
- **[ ] Emergency Access Procedure**
  - In the event of a power failure or fire, can authorized personnel still access data centers without compromising security?

SECTION 2: WORKSTATION USE & SECURITY (§ 164.310(b) & (c))

Can unauthorized eyes see patient data?

- **[ ] "Visual Hacking" Prevention**

  - Are monitors at nurse stations and registration desks positioned so that visitors/patients cannot view the screen?
  - *Test:* Stand in the public waiting area. Can you read the text on the receptionist's screen?
- **[ ] Unattended Workstation Protocols**
  - Do computers automatically lock after 3-5 minutes of inactivity?
  - *Physical Check:* Walk the floor during a shift change. Are any logged-in tablets or laptops left unattended on carts?
- **[ ] Physical Shielding**
  - Are privacy filters (polarized screen covers) installed on all monitors in high-traffic areas?

SECTION 3: VISITOR MANAGEMENT & SURVEILLANCE

Who is walking your halls?

- **[ ] The Vendor Log**
  - Is there a physical or digital log of every non-employee (vendor, delivery, family) who enters restricted areas?
  - *Requirement:* HIPAA requires you to track *who* was near the data and *when*.
- **[ ] Escort Requirements**
  - Are visitors allowed to walk unescorted to administrative offices?
  - *Best Practice:* Phoenix Officers provide "Visual Escort" or physical accompaniment for all vendors entering server rooms or records archives.
- **[ ] Camera Retention Policy**
  - Do your surveillance cameras retain footage for at least 30-90 days? (Crucial for investigating physical breaches of PHI).

SECTION 4: DEVICE & MEDIA CONTROLS (§ 164.310(d)(1))

How do you handle hardware disposal?

- **[ ] The "End of Life" Bin**
  - Is there a secured, locked bin for hard drives, flash drives, and backup tapes awaiting destruction?
  - *Risk:* Placing old hard drives in a standard open recycling bin is a guaranteed HIPAA violation.
- **[ ] Mobile Device Tracking**

- Is there a sign-in/sign-out log for shared tablets or medical devices used by nursing staff?

RISK SCORING

- **0 "No" Answers: Compliant.** Your physical defense strategy is sound.
- **1-3 "No" Answers: Moderate Risk.** You have gaps that could lead to a "Tier 2" HIPAA violation ($1,000 - $50,000 per violation).
- **4+ "No" Answers: High Risk.** Your facility is physically vulnerable. A stolen laptop or unescorted visitor could trigger a federal audit.

THE PHOENIX REMEDY

Security officers who understand Compliance.

We don't just stand guard; we enforce your HIPAA protocols.

- **Stationed Guards:** Enforce visitor logging and badge checks.
- **Mobile Patrols:** Check for unlocked workstations and unsecured record rooms during rounds.
- **Incident Reporting:** Digital documentation of every potential physical breach.