📅 Insider Threat Simulation Log Day 8: No BYOD Policy in Employee Handbook
Date of Entry: 6/23/2025
Observer: Michael Warner
Location: Organization-Wide (Policy Review)
Classification: Internal Security Simulation

🧾 Incident Overview

On the eighth day of my insider threat simulation, I reviewed the employee handbook and orientation materials and found that there is no formal policy addressing the use of personal devices (BYOD – Bring Your Own Device) in the workplace. This absence is especially troubling considering the organization handles Protected Health Information (PHI) and operates under HIPAA compliance requirements.

Employees frequently use personal smartphones, smartwatches, and in some cases, tablets during work hours — sometimes in close proximity to PHI and internal systems. Without a defined policy, there are no clear rules about data storage, app usage, or wireless connectivity on these devices.

⚠️ Risk Assessment

The lack of a BYOD policy introduces the following risks:

- Unsecured devices may store or transmit sensitive data without oversight
- No control over third-party applications or mobile device security posture
- Personal devices can be used to bypass company network protections
- Potential for unintentional HIPAA violations through photos, notes, or messaging apps

This represents a governance gap that places both employee behavior and organizational compliance at risk.

🕵️ Speculative Insider Perspective

As a malicious insider, I could:

- Use my personal device to photograph screens, documents, or patient records
- Record conversations or meetings involving confidential data
- Connect to internal systems or Wi-Fi networks and exfiltrate data unnoticed
- Leverage apps with cloud sync to silently transfer data offsite

Without formal restrictions or mobile device management, these actions would be difficult to detect or trace.

🛡️ Initial Thoughts & Actions

No devices were used for testing or interception. My analysis was based solely on policy review and observation of daily workplace behavior. This finding was logged without disruption or direct engagement.

✅ Recommendations (Low-Impact Suggestions)

- Draft and publish a BYOD policy that includes data protection requirements
- Implement Mobile Device Management (MDM) for personal device access to sensitive systems
- Provide employees with training on secure device usage and expectations
- Define consequences for unauthorized data access or sharing via personal devices
- Restrict camera and recording use in PHI-sensitive zones

🟠 Severity Rating

Moderate to High — depending on the volume of PHI handled and how often personal devices interact with sensitive areas.

- End of Entry -