📅 Insider Threat Simulation Log Day 6: Lobby File Exposure Before Transfer
Date of Entry: 6/21/2025
Observer: Michael Warner
Location: Front Lobby Area
Classification: Internal Security Simulation

🗒️ Incident Overview

On the sixth day of my insider threat simulation, I identified a temporary but concerning exposure of physical files containing PHI (Protected Health Information). These files are staged in boxes near the public-facing front lobby, awaiting transfer to the basement for long-term storage. This transfer is part of my regular job duties.

Typically, 1 to 2 boxes are present, though on rare occasions I've seen 3 or 4 stacked. While security cameras do cover the lobby area, they offer only post-incident review and do not physically prevent a potential breach. The boxes are sometimes left unguarded, meaning an individual could theoretically grab an entire box — or subtly remove individual documents — with minimal effort or scrutiny.

⚠️ Risk Assessment

Temporary exposure of PHI in public or semi-public spaces creates major risks:

- Unauthorized viewing, removal, or tampering of sensitive health data
- Increased potential for insider exploitation or casual theft
- Non-compliance with HIPAA or other data protection regulations
- Risk of reputational damage or legal penalties in the event of data loss

The presence of surveillance does not compensate for a lack of real-time control over physical files.

🕵️ Speculative Insider Perspective

As a malicious insider or opportunistic outsider, I could:

- Wait for the area to be briefly unattended and extract files from a box
- Walk out with an entire box
- Photograph records and return them without notice
- Leverage the incident to cause compliance violations or exfiltrate PHI for profit

The predictable routine of leaving files out front provides a repeatable window for exploitation.

🛡️ Initial Thoughts & Actions

For the purpose of fulfilling my regular duties I did move these boxes into storage as soon as I saw them. I recorded this behavior over several days during my normal work-related file transfers.

✅ Recommendations (Low-Impact Suggestions)

● Require files to be transferred directly from the front desk to the basement — no unattended staging
● Relocate temporary staging areas away from public-facing locations
● Instruct front desk staff to remain present when PHI boxes are awaiting pickup
● Use tamper-evident seals on boxes with sensitive data
● Establish written procedures for handling physical PHI transfers securely

🟠 Severity Rating

Moderate to High — the temporary nature lowers risk exposure duration, but the data sensitivity and location make it a notable vulnerability.

- End of Entry -